Ruijie RG-WLAN Series Wireless Controllers

RGOS Configuration Guide, Release 11.9(2)B2

Copyright Statement

Exemption Statement

Preface

Thank you for using our products. This manual matches the RGOS Release 11.9(2)B2.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://case.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.

{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols

Means reader take note. Notes contain helpful suggestions or references.

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

WLAN Basic Configuration

1. Configuring APMG
2. Configuring STA Management
3. Configuring CAPWAP
4. Configuring WBS
5. Configuring WLAN WBS FWD
6. Configuring ETH-MNG
7. Configuring DATA-PLANE
8. Configuring WLOG
9. Configuring Roaming

1 Configuring APMG

1.1 Overview

Tailored for the wireless network structures that support centralized management, AP Management (APMG) implements centralized management and configuration of access points (APs).

A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communication technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing terminals to move more flexibly.

A traditional WLAN adopts the fat AP network structure in which APs work independently. On the traditional WLAN, each AP must be separately configured and managed, which increases the complexity of network management and O&M workload. In addition, problems, such as radio interference between APs and roaming of wireless users, cannot be effectively resolved due to poor collaboration between APs. To address these issues, a wireless network structure that supports centralized management emerges. This network structure consists of access controllers (ACs) and fit APs, and is also called fit AP network structure. In this network structure, APs are connected to ACs through the Control and Provisioning of Wireless Access Points (CAPWAP), and ACs perform centralized management on APs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

1.2 Application

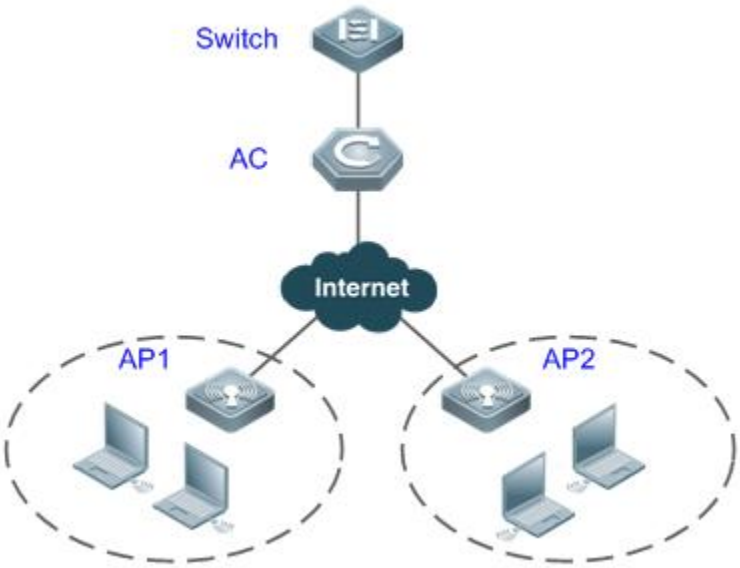
Application	Description
Fit AP Network Structure	This type of network consists of wired switches, ACs, and fit APs.

1.2.1 Fit AP Network Structure

Scenario

A fit AP network consists of wired switches, ACs, and fit APs. In the fit AP network structure, APs serve as the simple wireless access points and do not have the management or control function. The AC manages all the APs in a centralized manner, and pushes control policies to APs, and it is not necessary to configure APs one by one. As shown in Figure 1-1, the AC is connected to multiple APs through the CAPWAP tunnels. Users only need to perform configuration management on all the connected APs through the AC.

Figure 1-1 Simple fit AP network topology



Remarks	AP1 and AP2 are AP devices in fit AP mode.

Deployment

- Configure a meaningful name for each AP so that the AP can be configured based on the name.
- Create a WLAN and configure WLAN-related properties.
- Create an AP group and add APs to a specified AP group so that all the APs in this AP group can be configured in a centralized manner through the AP group.
- Deploy the WLAN on all the APs in the AP group through configuration of the AP group, after which the APs can provide the WLAN access service for external entities and wireless terminals users can access the WLAN.

1.3 Features

Basic Concepts

AP

AP is an access point used by wireless terminals to access a wired network. It is equivalent to a bridge for communication between wireless terminals and a wired network.

AC

AC is a wireless access controller. It is connected with APs through the wired network to manage and control APs in a centralized manner.

AC Cluster

AC cluster is also called AC redundancy. With this function, multiple ACs with different priorities are designated for an AP. When the connection between the AP and a high-priority AC is down, the AP is connected to a low-priority AC (standby AC). When the connection with the high-priority AC is recovered, the AP disconnects the CAPWAP tunnel with the low-priority AC, and sets up a CAPWAP tunnel with the high-priority AC again.

Overview

Feature	Description
Configuration of AC Authorization Key	Configure the license activation/deactivation key of an old version system.
Configuration of AC Parameters	Configure parameters, such as the AC name and Trap message control.
Configuration of AP Parameters	Configure parameters, such as the AP name, Telnet user name and password, and periodical statistics report interval.
Configuration of AP Behaviors	Configure AP behaviors, including daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.
AP Group Management	Manage APs through the AP group to reduce the workload incurred by configuring APs one by one.
AP Quantity Limit	Limit the maximum number of APs that can be connected to the AC.
AP Compliance Check	Implement the AP access control based on the bound MAC address.
AP Access Authentication	Authenticate the AP access.
AP Priority	Implement the AP access control based on the priority.
AC Cluster	Implement AC redundancy by using the AC cluster to reduce the AC single-point failure and improve availability of the wireless network.
AC Hot Backup	Set up the hot standby connection to ensure that the AP can set up two CAPWAP tunnels.
WLAN Configuration	Configure a WLAN and deploy the WLAN on APs to provide network services for wireless users.
AP Backup	Configure the AP backup function to improve availability of the wireless network.
AC Virtualization	Virtualize one AC into multiple ACs through permission control.
AP Virtualization	Virtualize an AP into multiple APs to be managed by different ACs.
Default SSID Configuration	Configure the default SSID of an AP. When no tunnel is available, the AP uses the default SSID to provide the WLAN access service.

1.3.1 Configuration of AC Authorization Key

The AC authorization key is a license activation key of an earlier version system, and used to control the upper limit of APs supported by an AC.

Working Principle

The license activation key is used to control the upper limit of APs supported by an AC. You can use a command to configure or add a valid license. The input license must be valid, effective, and applicable to the local device. If the upper limit of APs

supported by the AC is reached, no new license can be configured or added. You can also inactivate a license using the **no set license** *activation-key* command.

1.3.2 Configuration of AC Parameters

AC parameters include the AC name, Trap message control, and AC network access server (NAS) ID.

Working Principle

Configuration of AC parameters does not involve any working principle.

1.3.3 Configuration of AP Parameters

AP parameters include the AP name, Telnet user name and password, and periodical statistics report interval.

Working Principle

The AC configures AP parameters by pushing CAPWAP packets to an AP.

1.3.4 Configuration of AP Behaviors

AP behaviors include daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.

Working Principle

Configuration of AP behaviors is implemented by pushing CAPWAP packets to an AP. The AP performs the related behaviors based on the configuration pushed by the AC.

1.3.5 AP Group Management

The AC manages APs through the AP group. All the APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group. For the same configuration, if both the AP-based configurations and the AP-group-based configurations exist, the AP-based configurations prevail.

Working Principle

The system automatically creates a default AP group, which is named "default**"**. By default, APs are added to the default group. You can create AP groups and add APs to these groups to manage APs by group.

1.3.6 AP Quantity Limit

The maximum number of APs that can be connected to an AC is configured to limit the maximum AP load of the AC, thus avoiding overload of the AC.

Working Principle

When the number of APs connected to the AC reaches the maximum number, no more APs can access the AC.

For the WALL-AP product series supplied by Ruijie Network, each device is treated as 0.5 device when the maximum number of APs that can be connected to an AC is calculated. That is, the maximum number of WALL-APs that can be connected to an AC is twice the number of APs supported by the AC.

1.3.7 AP Compliance Check

The AP compliance check is also called AP access control based on the bound MAC address. If the AP compliance check is enabled, only APs with some specified MAC addresses are allowed to access the AC. This prevents access of unwanted APs and enhances security of the wireless network.

Working Principle

An AP is allowed to access the AC only when the AP configuration that is bound with the MAC address of this AP exists on the AC; otherwise, access of the AP to the AC is denied. To prevent binding MAC addresses with a large number of AP configurations, the MAC addresses of currently online APs are automatically bound when the AP compliance check is enabled. In addition, MAC addresses can be bound with specified AP configurations.

1.3.8 AP Access Authentication

AP access authentication can be implemented based on the serial number, password, or certificate. With the AP access authentication function, only authorized APs can access the AC.

Working Principle

When an AP sends an access request to the AC and uploads the authentication information, the AC verifies the authentication information. Only the AP that is successfully authenticated can access the AC.

1.3.9 AP Priority

The AP priority function is an advanced version of the AP quantity limit function. With this function, when the current number of APs connected to the AC reaches the upper limit, if a high-priority AP sends an access request, the AC proactively forces a low-priority AP to go offline and allows the access of the high-priority AP.

Working Principle

When an AP sends an access request, the current number of APs connected to the AC reaches the upper limit, and the AP priority function is enabled, the AC first compares the priorities. If the priority of an online AP is lower than the requesting AP, the AC forces a low-priority AP to go offline and allows the access of the high-priority AP.

1.3.10 AC Cluster

On the one hand, the AC cluster function enhances reliability of the AC cluster. On the other hand, this function controls the home AC of APs in stable conditions based on the priority to facilitate AP management.

Working Principle

See the CAPWAP protocol in RFC5415.

1.3.11 AC Hot Backup

The AC hot backup function is a dual-host hot standby function. It enables switchover of the CAPWAP tunnels between ACs and APs within several milliseconds when an AC is unreachable or faulty, thus ensuring uninterrupted services for associated STAs to the maximum extent.

Working Principle

Two tunnels are set up between an AP and two ACs, and one tunnel works in active mode, and the other works in standby mode. The AC corresponding to the active tunnel serves as the active device that processes all services and transfers the service status information to the standby device for backup purpose. The standby device does not process services, and only backs up the service data. If the active AC is faulty, the standby AC takes over all services.

For details about AC hot standby, see "Configuring WLAN Hot Standby".

1.3.12 WLAN Configuration

Create and deploy a WLAN on an AP so that the AP can provide the WLAN access service for external entities.

Working Principle

The WLAN created on the AC is used for WLAN parameter configuration. The WLAN deployment information and parameters are pushed through the packets defined in the CAPWAP protocol.

1.3.13 AP Backup

The AP backup function is used to back up radio signals transmitted by APs that are physically adjacent with each other, have overlapped coverage, and transmit different radio signals. When an AP that transmits important radio signals is faulty, one or more standby APs transmit radio signals of the faulty AP to replace the faulty AP, thus ensuring stability of radio signals transmitted by devices supplied by Ruijie Networks. This function is generally used in special scenarios. For example, in the zero roaming scenario of the medial industry, the AP4210 with a wide coverage is an important AP, and the APD-M within the coverage of the AP4210serves as a standby AP of the AP4210.

Working Principle

An AP backup group is created on the AC. In this AP backup group, one AP is selected as the active AP, and other APs are standby APs. When the active AP is faulty and goes offline, the WLAN configuration of the active AP is sent to all the standby APs in the group so that the standby APs can transmit radio signals of the active AP.

1.3.14 AC Virtualization

AC virtualization function is used to virtualize one AC into multiple ACs through permission control. Currently, AC virtualization function takes effect only to web management. Users can log in to the web management page using different administrator accounts to check and configure different WLANs, AP groups, and APs. In addition, administrators can back up information of each other. When multiple administrators share the same role, these administrators have the same permissions. When one administrator cannot perform operations due to absence or other causes, another administrator can log in to the web management page using his or her own account and perform the operations. This ensures account security.

Working Principle

A super administrator can create different roles on the AC or by logging in to the web management page, associate administrators with different roles, and assign WLANs, AP groups, and APs to the roles. When an administrator logs in to the web management page, the administrator can only check and configure the corresponding WLANs, AP groups, and APs (STAs). This ensures that different roles manage the same AC at the same time but do not interfere with each other, achieving the effect of virtualizing one AC into multiple ACs.

1.3.15 AP Virtualization

The AP virtualization function virtualizes one AP into multiple APs. Each virtual AP establishes a connection to an AC (not in the hot backup state), and these virtual APs share physical resources of the AP. Each AC can deliver its own configurations and configure its own wireless signals to manage the AP. When an STA receives signals released by an AC, the AP serving the STA reports the corresponding data to the AC. As the data channels used by the virtual APs to report data to the ACs are different and the virtual APs are not accessible to each other, the data security is improved. In addition, as the APs are controlled by multiple ACs, the AC single point of failure (SPOF) will not occur and the AP stability is improved.

Working Principle

Create an AP virtualization template on the active AC and apply the template to an AP, an AP group, or all APs. In this case, the AP establishes connections to other ACs according to configurations of the AP virtualization template and the connected ACs can deliver their own configurations to the AP.

1.3.16 Default SSID Configuration

Configure an SSID for a fit AP to provide the WLAN access service when no CAPWAP tunnel is established.

Working Principle

The AC configures a default SSID for the AP. When the AP restarts or the tunnel is torn down, the AP uses the SSID to provide the WLAN access service.

1.4 Configuration

Configuration	Description and Command	
Configuring the AC Authorization Key	⚠ (Optional) To increase the number of APs supported by an AC, purchase and install a new license.	
	set license	Configures the license activation key.
	license-idle-timeout	Configures the shared aging time of a license.
Configuring an AC Name	⚠ (Optional) A meaningful name can be configured for the AC to facilitate management.	
	ac-name	Configures the name of the local AC.

Configuration	Description and Command	
Configuring the Trap Message Control Function	(Optional) It is used to enable sending of Trap messages. Network operation and maintenance (O&M) can be implemented based on the received Trap messages.	
	acctrl-trap	Configures whether the AC sends specified Trap messages.
Configuring the NAS ID of an AC	(Optional) By default, the NAS ID is the MAC address of the AC in dotted decimal notation.	
	nas-id	Configures the NAS ID of the AC in AC configuration mode.
Creating an AP Configuration	(Optional) It is used to create an AP configuration to configure a specified AP.	
	ap-config	Adds an AP configuration, or enter the AP configuration mode.
Creating an AP Group	(Optional) In AP group configuration mode, this command takes effect on all the online APs in the AP group.	
	ap-group	Adds an AP group configuration, or enters the AP group configuration mode.
Configuring the AP Group of an AP	(Optional) It is used to configure the AP group of a specified AP in AP configuration mode. By default, an AP belongs to the default group.	
	ap-group	Configures the AP group of an AP.
Configuring an AP Name	(Optional) A new name can be configured for an AP according to requirements.	
	ap-name	Configures an AP name.
Binding an MAC Address with an AP Configuration	(Optional) It is used to bind an MAC address with an AP configuration so that the AP configuration can take effect on the AP with the MAC address.	
	ap-mac	Binds an MAC address with an AP configuration.
Configuring the User Name and Password of an AP	(Optional) It is used to modify the Telnet user name and password of an AP according to requirements.	
	credential	Configures the user name and password of an AP.
Configuring the Interval at Which the AP Reports Statistics	(Optional) According to the standard, the AP reports statistics at the interval of 120s by default. The interval can be configured according to requirements.	
	statistics-timer	Configures the interval at which the AP reports statistics.
Configuring the Daily Scheduled Restart Time for an AP	(Optional) The daily scheduled restart function can be configured for an AP to prevent the AP from working for a long time.	
	reload at	Configures the daily scheduled restart time for an AP.
	(Optional) It is used to restore factory settings of an AP.	

Configuration	Description and Command	
Restoring Factory Settings of a Specified AP	**factory-reset**	Restores factory settings of a specified AP.
Resetting an AP	(Optional) It is used to reset an AP.	
	reset	Resets an AP.
Configuring the AP Quantity Limit	(Optional) The maximum number of APs connected to the AC can be configured according to requirements to reduce the maximum load of the AC.	
	wtp-limit	Configures the maximum number of APs that can be connected to the AC.
Configuring the AP Compliance Check	(Optional) The AP compliance check can be enabled to allow the access of only APs with the bound MAC addresses, thus effectively controlling the access of APs.	
	bind-ap-mac	Enables or disables the AP compliance check in AC configuration mode.
Configuring AP Access Authentication	(Optional) AP access authentication can be configured so that only authorized APs can access the AC, which enhances security of the wireless network.	
	ap-auth enable	Enables or disables the AP access authentication function of the AC in AC configuration mode.
	ap-auth serial-update	Updates authentication serial numbers for all online APs in AC configuration mode.
	ap-auth	Configures the access authentication information of an AP in AP configuration mode.
Configuring the AP Priority	(Optional) This command is available in both the AC and AP configuration modes.	
	ap-priority	Enables or disables the AP access priority function of the AC in AC configuration mode.
	priority	Configures the failover priority of a specified AP in AP configuration mode.
Configuring the AC Cluster Function	(Optional) It is used to configure the redundancy ACs of a specified AP or all APs in AP configuration mode.	
	primary-base	Configures the primary AC of an AP.
	secondary-base	Configures the secondary AC of an AP.
	tertiary-base	Configures the tertiary AC of an AP.
	backup-controller-primary	Configures the fourth AC of an AP.
	backup-controller-secondary	Configures the fifth AC of an AP.
	backup-controller-tertiary	Configures the sixth AC of an AP.
	(Optional) It is used to adjust the hot backup connection parameters.	

Configuration	Description and Command	
Configuring the AC Hot Backup Function	**ap-group**	Binds an AP group.
	peer-ip	Configures the peer IP address.
	peer-ipv6	Configures the peer IPv6 address.
	peer-ipv6 enable	Enables the peer IPv6.
Configuring the AP System Log Information	(Optional) It is used to configure the log information of a specified AP or all APs in AP configuration mode.	
	logging on	Enables or disables the function of displaying system logs.
	logging server	Configures the address of the system logging server.
Creating a WLAN	(Optional) A WLAN must be created before it can be deployed.	
	wlan-config	Creates a WLAN, or enters the WLAN configuration mode.
Deploying a WLAN	(Optional) It is used to configure the WLAN-VLAN mapping of a specified AP group and deploy the WLAN on all the APs in the AP group.	
	interface-mapping	Configures the WLAN-VLAN mapping of a specified AP group in AP group configuration mode.
Enabling or Disabling WLAN SSID Broadcasting	(Optional) SSID broadcasting is disabled by default.	
	enable-broad-ssid	Enables or disables SSID broadcasting of a specified WLAN in WLAN configuration mode.
Configuring the NAS ID of WLAN Users	(Optional) The NAS ID is a null string by default.	
	nas-id	Configures the NAS ID of a specified WLAN user.
Configuring the Fit or Fat AP Mode	(Optional) The AP mode can be switched between the fit AP mode and the fat AP mode according to requirements.	
	switch2fat	Switches the mode of a specified AP to the fat AP mode in AC configuration mode on the AC device.
	ap-mode	Configures the fit or fat AP mode in global configuration mode.
Configuring the WLAN SSID Name	(Optional) A new SSID can be configured for the WLAN according to requirements.	
	ssid	Modifies the SSID name of the WLAN in WLAN configuration mode.
	ssid-code	Configures the coded character set for the SSID.
Configuring the AP Backup Function	(Optional) It is used to improve availability of the wireless network.	
	ap-backup group	Creates an AP backup group in AC configuration mode.
	ap-backup-group	Binds an AP backup group.

Configuration	Description and Command	
Configuring the AC Virtualization Function	(Optional) It is used to assign wireless permissions and virtualize one AC into multiple ACs.	
	permit enable	Configures whether to enable AC virtualization
	master-group	Adds a role and enters the role configuration mode.
	master-group (AP configuration mode)	Assigns an AP to a specific role in AP configuration mode.
	master-group (AP group configuration mode)	Assigns an AP group to a specific role in AP group configuration mode.
	master-group (WLAN configuration mode)	Assigns a WLAN to a specific role in WLAN configuration mode.
	webmaster (role configuration mode)	Adds/Deletes an administrator in role configuration mode.
Configuring the AP Virtualization Function	(Optional) It is used to enable multiple ACs to manage the same AP.	
	virtual-ap	Creates an AP virtualization template in global configuration mode.
	ac-ip	Configures the IP address of the AC to which a virtual AP is to be connected.
	wlan-capacity	Configures the number of WLANs supported by a virtual AP.
	sta-capacity	Configures the number of STAs supported by a virtual AP.
	link-interface	Configures the uplink interface used by a virtual AP to connect to an AC.
	virtual-ap	Configures a virtual AP in single AP, AP group, and all-AP configuration modes.
	ap-idle-timeout	Configures the duration for a virtual AP to continue service provision after the connection between the AP and active AC is down.
Configuring the Default SSID	**offline-ssid**	Configures the WLAN access signal provided when an AP is offline.

1.4.1 Configuring the AC Authorization Key

Configuration Effect

- Increase the number of APs supported by an AC.

Notes

- A configured license takes effect permanently. That is, the license never expires. Once you configure the license, you are assigned to use the function permanently.

- The license takes effect as soon as it is configured on a device, and restart of the device is not necessary.
- Multiple licenses can be configured on the same AC device. That is, the maximum number of APs supported by an AC is equal to the sum of the AP quantities authorized by the licenses, but cannot exceed the capacity of the AC.
- After being inactivated, the license cannot be installed on the device again. But you can apply for a new license for another device using this license, the old SN, the deactivation key and a new SN.
- After you inactivate a license, the number of APs allowed to be online reduces immediately. The APs that are already online are not affected.
- This command is used to import the activation key of the earlier-version license system. A new license is installed by using the license file installation command. For details, see "Software Authorization Management."

Configuration Steps

- Optional. To increase the number of APs supported by an AC, purchase and install a new license.
- The license activation key is not installed by default.
- You can run the **set license** *activation-key* command in global configuration mode to import the activation key of the earlier-version license system.
- You can run the **no set license** *activation-key* command in global configuration mode to inactivate an existing activation key.

Command	**set license***activation-key*
Parameter Description	*activation-key*: indicates the license activation key to be configured. The format of the license key depends on the actual situations, for example, AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A license is applicable to only the device that you specify when applying for a license, and does not take effect on other devices. The same license cannot be configured for multiple times on one device.

Command	**no set license** *activation-key*
Parameter Description	*activation-key*: indicates the license key to be inactivated. The format of the license key depends on the actual situations, for example, AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	After being inactivated, the license cannot be installed on the device again. But you can apply for a new license for another device using this license, the old SN, the deactivation key and a new SN.

Command	**license-idle-timeout** *timeout*
Parameter Description	*timeout*: Indicates the shared aging time (in the unit of hour) of the license in a license sharing network after the AC stops using the license. The value ranges from **1** to **336** (14 days).

Defaults	168 (7 days)
Command Mode	AC configuration mode
Usage Guide	This command applies to the license sharing scenarios, for example, AC virtualization scenarios.

Verification

- Run the **show license all-license** command to check the license information and determine whether the configuration is successful.
- **show license unbind-code command** to check the inactivated license.

Configuration Example

Configuring the License Activation Key

Configuration Steps	• Add a license.
AC	`Ruijie#config terminal` `Ruijie(config)#set license4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA`
Verification	Run the **show license all-license** command to check the current license.
AC	`Ruijie(config)#show license all-license` `Searching license in the system...` `There's no license installed in the system.` `-----------------------------------------` `There are some old version licenses:` `1. 4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA 128`

Inactivating a License

Configuration Steps	• Inactivate a license.
AC	`Ruijie#config terminal` `Ruijie(config)# no set license 4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA` `After unbinding, you can not install the corresponding license again. Are you sure to continue[y/n]:y` `The verification string is: xxxxxxxxxxxx`

Verification	Run the **show license all-license** command to check the inactivated license.
AC	`Ruijie(config)#show license unbind-code` `LICENSE UNBINDING-CODE` `4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA xxxxxxxxxxxxxxxxxxxxxxxxxxxx`

Common Errors

- N/A

1.4.2 Configuring an AC Name

Configuration Effect

- Set the name of an AC to a specified string.

Notes

- The AC name is a string of 1 to 63 characters, and cannot contain any space.

Configuration Steps

- Optional. Run the **ac-name** *ac-name* command in AC configuration mode to configure a new name for an AC.
- Run the **ac-controller** command to enter the AC configuration mode.
- Run the **ac-name** command to configure an AC name in AC configuration mode on an AC device.

Command	**ac-controller**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ac-name***ac-name* **no ac-name**
Defaults	The default AC name is Ruijie_Ac_*Last six digits of MAC address*. For example, if the MAC address of an AC is 001a.a916.e7b8, the default name of this AC is Ruijie_Ac_16e7b8.
Parameter Description	*ac-name*: indicates the name of an AC. The name is a string of 1 to 63 characters, and cannot contain any space.
Command Mode	AC configuration mode
Usage Guide	Different names can be configured for different ACs to facilitate management.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

↘ Configuring the Name of an AC as "Ruijie-AC1"

Configuration Steps	● Enter the AC configuration mode. ● Configure an AC name. ● Use the **no** form of this command to restore the default AC name.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#` `Ruijie(config-ac)#ac-name Ruijie-AC1` `Ruijie(config)#ac-controller` `Ruijie(config-ac)#no ac-name`
Verification	Run the **show ac-config** command to check the current AC name.
AC	`Ruijie#show ac-config` `ac_name :Ruijie-AC1`

Common Errors

- N/A

1.4.3 Configuring the Trap Message Control Function

Configuration Effect

- The AC sends the following types of Trap messages: CAPWAP tunnel up/down information, failures to add APs to the AC,CAPWAP tunnel packet decryption failures, upgrade failures, time synchronization failures, and STA online/offline information.
- By default, all the preceding Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable sending of specified Trap messages.

Notes

- N/A

Configuration Steps

- Optional. On the AC device, enter the AC configuration mode and run the **acctrl-trap** command to configure the Trap message control function.

Command	**acctrl-trap**[**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]
Parameter Description	**acap-updown-ctrl**: Determines whether to send the Trap messages that contain the CAPWAP tunnel up/down information. **acap-joinfail-ctrl**: Determines whether to send the Trap messages that contain information about failures of adding APs to the AC. **acap-decryeroreport-ctrl**: Determines whether to send the Trap messages that contain information about CAPWAP tunnel packet decryption failures. **acap-imageupdt-ctrl**: Determines whether to send the Trap messages that contain information about the **bin** file upgrade failures of the AP. **acap-timestamp-ctrl**: Determines whether to send the Trap messages that contain the time synchronization information. **acsta-oper-ctrl**: Determines whether to send the Trap messages that contain the STA online/offline information.
Defaults	By default, all types of Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable sending of these messages.
Command Mode	AC configuration mode
Usage Guide	This command is used to control sending of Trap messages on the AC.

Verification

- Run the **show ac-config** command to check the sending status of various types of Trap messages.

Configuration Example

↘ Enabling the AC to Send the Trap Messages That Contain Information About Failures to Add APs to the AC

Configuration Steps	• Enter the AC configuration mode. • Enable the AC to send the Trap messages that contain information about failures to add APs to the AC. • Use the **no** form of this command to restore the default setting.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#acctrl-trap acap-joinfail-ctrl` `Ruijie(config)#ac-controller` `Ruijie(config-ac)#no acctrl-trap acap-joinfail-ctrl`
Verification	Run the **show ac-config** command to check the sending status of various types of Trap messages.

AC	Ruijie#show ac-config acctrl-trap acap-updown-ctrl :Disable acctrl-trap acap-joinfail-ctrl :Enable acctrl-trap acap-decryeroreport-ctrl :Disable acctrl-trap acap-imageupdt-ctrl :Disable acctrl-trap acap-timestamp-ctrl :Disable acctrl-trap acsta-oper-ctrl :Disable

Common Errors

- N/A

1.4.4 Configuring the NAS ID of an AC

Configuration Effect

- On the WLAN, the NAS IDs identify different hot spot areas. By default, the NAS ID of an AC is the MAC address of the AC in dotted decimal notation.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the AC configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *ac-nas-id* **no nas-id**
Parameter Description	N/A
Defaults	MAC address of the AC in dotted decimal notation
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check the AC configuration.

Configuration Example

Setting the NAS ID of the AC to 123456789

Configuration Steps	● Enter the AC configuration mode. ● Configure the NAS ID.
AC	`Ruijie(config)# ac-controller` `Ruijie(config-ac)#nas-id123456789`
Verification	Run the **show running** command to check the AC configuration.
AC	`Ruijie#show running` `!` `ac-controller` ` nas-id 123456789` `!`

Common Errors

- N/A

1.4.5 Creating an AP Configuration

Configuration Effect

- Create an AP configuration with the specified name, and enter the AP configuration mode.
- If the AP configuration corresponding to a name already exists, you can directly enter the AP configuration mode after the command is executed.
- The *ap-name* parameter indicates the name of the AP configuration. When an AP gets online, the AP name uploaded by the AP is matched with the AP configuration name to determine the mapping relationship between the AP device and AP configuration.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the global configuration mode and run the **ap-config***ap-name* command to create an AP configuration.

Command	**ap-config** *ap-name*
Parameter Description	*ap-name*: indicates the name of the AP configuration.

Defaults	No AP configuration is created by default.
Command Mode	Global configuration mode
Usage Guide	1. You can run the **ap-config all** command to enter the all-AP configuration mode. Configurations made in this mode take effect on all APs associated with the current AC. Configurations made in AP configuration mode take precedence over configurations made in all-AP configuration mode. If configurations (non-default settings) exist in AP configuration mode (entered by running the **ap-config** *ap-name* command), such configurations are preferentially used; otherwise, configurations made in all-AP configuration mode (entered by running the **ap-config all** command) are used. 2. You can run the **no ap-config** *ap-name* command to delete a specified AP configuration. If the AP corresponding to this configuration is already online, the AP will be forced offline and then go online again after the configuration is deleted. 3. You can run the **no ap-config all** command to delete configurations of all offline APs on the current AC.

Verification

- Run the **show ap-config running** *ap-name* command to check the configurations of the AP.

Configuration Example

Creating an AP Configuration Named "Ruijie_AP"

Configuration Steps	• Create an AP configuration named "Ruijie_AP".
AC	`Ruijie(config)#ap-config Ruijie_AP` `You are going to config AP(Ruijie_AP), which is not on line now.` `Ruijie(config-ap)#`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie#show ap-config running Ruijie_AP` `!` `ap-config Ruijie_AP` `!`

Common Errors

- N/A

1.4.6 Creating an AP Group

Configuration Effect

- The AC manages APs through the AP group. All the APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group.

Notes

- The default group is created automatically by the system, and cannot be deleted.
- When an AP group is deleted, APs of this group are automatically moved to the default group.
- Configurations made in different configuration modes take effect in the following sequence: ap-config ap-name>ap-group>ap-config all.

Configuration Steps

- Optional.
- On the AC device, enter the global configuration mode, and run the **ap-group** *ap-group-name* command to create an AP group.

Command	**ap-group** *ap-group-name* **no ap-group** *ap-group-name*
Parameter Description	***ap-group-name***: indicates the name of an AP group.
Defaults	An AP group named "default" is automatically created by default after the system is started. This group can neither be created nor deleted.
Command Mode	Global configuration mode
Usage Guide	When the **no** form of the command is used to delete an AP group, APs of this group are automatically moved to the default group.

Verification

- Run the **show running** command to check configurations of all AP groups.

Configuration Example

↘ Creating an AP Group Named "APG-1"

Configuration Steps	● In global configuration mode, run the **ap-group** command to create an AP group.
AC	`Ruijie(config)#ap-group APG-1` `Ruijie(config-ap-group)#`
Verification	Run the **show running** command to check whether the AP group named "APG-1" exists.

AC	Ruijie#show running ! ap-group APG-1 !

Common Errors

- N/A

1.4.7 Configuring the AP Group of an AP

Configuration Effect

- An AP group must already exist if you want to add an AP to this group.
- By default, APs belong to the default AP group, that is, the AP group named "default".
- APs inherit all configurations of the AP group to which APs belong. If the same configuration exists in the specified AP configurations (**ap-config***ap-name*), all AP configurations (**ap-config all**), and AP group configurations, the configurations take effect in the following sequence: specified AP configurations > AP group configurations > all AP configurations. Therefore, if the AP group of an AP changes, AP group configurations inherited by this AP change as well.

Notes

- N/A

Configuration Steps

- Optional.
- Run the **ap-config** command to create an AP group or enter the AP configuration mode.
- On the AC device, enter the AP configuration mode and run the **ap-group** command to configure the AP group of an AP.

Command	**ap-config***ap-name*
Parameter Description	*ap-name***:** indicates the name of the AP configuration.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ap-group** *ap-group-name* **no ap-group**
Parameter Description	*ap-group-name***:** indicates the name of an AP group.

Defaults	By default, APs are automatically added to the default group.
Command Mode	AP configuration mode
Usage Guide	When an AP group is deleted, APs of this group are automatically moved to the default group.

Verification

- Run the **show ap-config running** command to check the current configurations of the AP.

Configuration Example

Configuring the AP Group to Which Ruijie-AP1 Belongs

Configuration Steps	• Create an AP group named "apg-1". • Enter the AP configuration mode. • Use the **no** form of this command to restore the default AP group, that is, the AP group named "default".
AC	`Ruijie(config)#ap-group apg1` `Ruijie(config-ap-group)#` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#` `Ruijie(config-ap)#ap-group apg-1` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ac)#no ap-group`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `ap-group apg-1` `!`

Common Errors

- N/A

1.4.8 Configuring an AP Name

Configuration Effect

Configure an AP name on the AC.

- If the AP is currently online, the configuration of the AP name takes effect immediately. In addition, the AP name in the specified AP configuration mode (that is, the string next to **ap-config**) is immediately replaced by the new name.
- If the AP is currently offline, the configuration of the AP name takes effect after the AP goes online, and the AP name in the AP configuration mode is not replaced by the new name until the AP goes online.
- After the AP name is configured, you can continue to configure this AP without exiting from the AP configuration mode.
- If the corresponding AP is online, the **no** form of the command is not supported.
- If the corresponding AP is online, the **no** form of the command can be used to delete the AP name configuration that is currently not effective.
- If the new name is already in use, the configuration fails.

Configure an AP name on the AP.

- If the CAPWAP connection is not set up, the AP name is configured directly.
- If the CAPWAP connection is set up, the AP name is configured first. Then the CAPWAP tunnel will be torn down and a connection will be set up again. If the AP name is already configured on the AC or configured offline, this AP name prevails.

Notes

- The AP name is a string of 1 to 63 characters, and cannot contain any space.
- The AP name cannot be configured as "all" or "AP".
- Avoid configuring the same AP name for different offline APs. If the same AP name is configured for different offline APs, the new name takes effect on the AP that goes online first, and the APs that go online later still use the original names.
- Configuring the AP name on the AP only takes effect in fit AP mode.

Configuration Steps

- Optional. You can run the **ap-name** *ap-name* command in AP configuration mode to configure an AP name. It is recommended that a meaningful AP name be configured to facilitate management.
- On the AC device, enter the AP configuration mode and run the **ap-group** command to configure an AP name.

Command	**ap-name** *name*
Parameter Description	*name*: indicates the name of an AP. The name cannot contain any space.
Defaults	The AC uses the name uploaded by the AP as the AP name. In the factory settings, the MAC address is often used as the name of an AP.
Command Mode	AP configuration mode
Usage Guide	1. Do not configure the AP name as "all" or "AP". 2. After the command is executed, the command mode of an online AP is the AP command mode with the new AP name, and you can continue to configure other properties of the AP without existing from the command mode. The command mode of an offline AP remains unchanged.

- On the AP device, enter the global configuration mode and run the **ap-name** command to configure an AP name.

Command	**ap-name** *name*
Parameter Description	*name*: indicates the name of an AP. The name cannot contain any space.
Defaults	The default name is AP.
Command Mode	Global configuration mode
Usage Guide	1. Do not configure the AP name as "all". 2. After this command is executed, the CAPWAP tunnel will be set up again.

Verification

- Run the **show ap-config running** command to check the current configurations of the AP.
- Run the **show ap-config summary** command to check whether the name of the online AP is the new name.
- Run the **show running-config** command to check the AP configuration.

Configuration Example

Changing the Name of an Online AP from "Ruijie-AC1" to "Ruijie-AC2"

Configuration Steps	• Enter the AP configuration mode. • Configure the name of an AP.
AC	`Ruijie(config)#ap-config Ruijie-AC1` `Ruijie(config-ap)#ap-name Ruijie-AC2`
Verification	• Run the **show ap-config running** command to check the current configurations of the AP. • Run the **show ap-config summary** command to query the current name of the online AP.
AC	`Ruijie#show ap-config running` `!` `ap-config Ruijie-AC2` `!` `Ruijie#show ap-config summary` `========= show ap status =========` `Radio: Radio ID or Band: 2.4G = 1#, 5G = 2#` `E = enabled, D = disabled, N = Not exist` `Current Sta number/Max Sta number supported` `Channel: * = Global`

```
      Power Level = Percent


Online AP number: 0

Offline AP number: 1


AP Name                                 IP Address      Mac Address    Radio 1
Radio 2           Up/Off time   State
---------------------------------------- --------------- -------------- -----
-------------- ------------------ ------------- -----

ap1                                  10.0.20.15     00d0.f822.33b0 N   -/-     -
- N   -/-     -     -    0:00:16:03 Quit
```

Changing the Name of an Offline AP from "Ruijie-AC1" to "Ruijie-AC2"

Configuration Steps	● Enter the AP configuration mode. ● Configure the name of an AP.
AC	`Ruijie(config)#ap-config Ruijie-AC1` `Ruijie(config-ap)#ap-name Ruijie-AC2`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie#show ap-config running` `!` `ap-config Ruijie-AC1` `  ap-name Ruijie-AC2` `!`

Deleting the Name Configuration of an Offline AP Ruijie-AC1

Configuration Steps	● Enter the AP configuration mode. ● Delete the name configuration of an offline AP Ruijie-AC1.
AC	`Ruijie(config)#ap-config Ruijie-AC1` `Ruijie(config-ap)#no ap-name`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie#show ap-config running` `!`

	ap-config Ruijie-AC1 !

Configuring the Name of an AP as Ruijie-AP1.

Configuration Steps	● Enter the global configuration mode. ● Configure the AP name.
AP	Ruijie(config)#ap-name Ruijie-AP1
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AP	Ruijie#show running-config Building configuration... Current configuration: 1592 bytes version 11.1(5)B0 privilege exec all level 1 debug privilege exec all level 1 show privilege exec all level 1 terminal privilege exec all level 1 undebug ap-name Ruijie-AP1 fair-schedule !

Common Errors

- N/A

1.4.9 Binding an MAC Address with an AP Configuration

Configuration Effect

- In AP configuration mode, run the **ap-mac** command to bind an MAC address with an AP configuration so that the AP configuration takes effect only on the AP with the MAC address.
- Generally, when an AP goes online, it determines the configuration to be used based on the mapping between the AP name and the AP configuration name. MAC address binding is a stronger binding relationship than name mapping, and takes precedence over name mapping. Therefore, when an AP goes online, the AP uses the configuration so far as the MAC address bound with the AP configuration is the same as the MAC address of the AP.
- If no MAC address is bound with an AP configuration, the MAC address is automatically bound when the corresponding AP goes online. This bounding relationship still takes effect when the AP goes offline. That is, the binding configuration will be automatically generated when the AP goes online.

- MAC address binding is also used for the AC access control function configured by using the **bind-ap-mac** command. For details, see the configuration description of this command.
- You can bind a specified MAC address only with the configuration of an offline AP.
- In the hot standby environment, you can ensure consistency of configurations between two ACs by binding the MAC addresses with AP configurations.

Notes

- You can bind a specified MAC address only with the configuration of an offline AP.

Configuration Steps

- Optional.
- On the AC device, enter the AP configuration mode and run the **ap-mac** command to bind an MAC Address with an AP configuration.

Command	**ap-mac** *ap-mac-address* **no ap-mac**
Parameter Description	*ap-mac-address*: indicates the MAC address that is bound.
Defaults	No AP configuration is bound with the MAC address by default. You can bind the MAC address of an AP with the AP configuration to forcibly apply this AP configuration on the AP with the MAC address.
Command Mode	AP configuration mode
Usage Guide	● The **ap-mac** *ap-mac-address* command is applicable to configurations of offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online. ● The **no ap-mac** command is applicable to all AP configurations.

Verification

- Run the **show ap-config running** command to check the MAC address binding of the current AP.

Configuration Example

↘ Binding the Offline AP Ruijie-AP1 with the MAC Address 001a.a979.1234

Configuration Steps	● Enter the AP configuration mode. ● The **no** form of the command is used to delete the MAC address binding.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#ap-mac 001a.a979.1234` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ac)#no ap-mac`

Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  ap-mac 001a.a979.1234` `!`

Common Errors

- N/A

1.4.10 Configuring the User Name and Password of an AP

Configuration Effect

- Authorized users may directly login to an AP and modify the AP configuration through Telnet, which affects normal running of the WLAN. To prevent this problem, you can configure the Telnet user name and password of a specified AP.
- The **credential** command can be used in **ap-config** *ap-name*, **ap-group**, or **ap-config all** configuration mode. Configurations made by using the **credential** command take effect in the following sequence: **ap-config** *ap-name*>**ap-group**>**ap-config all**.

Notes

- N/A

Configuration Steps

- Optional: You can run the **credential** *user-name password* command to configure a new Telnet user name and password in AP configuration mode to enhance security.
- On the AC device, enter the AP or AP group configuration mode and run the **credential** command for configuration.

Command	**credential** *user-name password* **nocredential**
Parameter Description	*user-name*: indicates the user name. A user name cannot contain any space. *password*: indicates the password. A password cannot contain any space.
Defaults	The AC device uses factory settings of the Telnet user name and password of an AP. You can modify the Telnet user name and password of an AP according to requirements to facilitate management.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** or **show running** command to check the configurations.

Configuration Example

Configuring the User Name and Password of Ruijie-AP1

Configuration Steps	● Configure the user name and password of Ruijie-AP1. ● Use the **no** form of the command to delete the configuration of the user name and password of the AP. (After the deletion, the default user name and password are restored on the AP.)
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#credential user pass` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ac)#no credential`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  credential user pass` `!`

Common Errors

- N/A

1.4.11 Configuring the Interval at Which the AP Reports Statistics

Configuration Effect

- Run the **statistics-timer** command to configure the interval at which the AP reports statistics.

Notes

- N/A

Configuration Steps

- Optional. You can adjust the interval based on the statistics accuracy requirement and loads on the AC and AP.
- On the AC device, enter the AP or AP group configuration mode and run the **statistics-timer** command for configuration.

Command	**statistics-timer** *timer-interval* **nostatistics-timer**
Parameter Description	*timer-interval*: indicates the interval that the AP reports statistics. The unit is second.
Defaults	120s

Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

Setting the Interval at Which Ruijie-AP1 Reports Statistics to 300s

Configuration Steps	• Set the interval at which Ruijie-AP1 reports statistics to 300s. • Use the **no** form of the command to restore the default interval at which Ruijie-AP1 reports statistics.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#statistics-timer 300` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ac)#no statistics-timer`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  statistics-timer 300` `!`

Common Errors

- N/A

1.4.12 Configuring the AP System Log Information

Configuration Effect

- Control displaying of the AP system logs, and set the IP address of the server that records the AP system logs.

Notes

- N/A

Configuration Steps

- Optional.
- Run the **logging on** command to display system logs of a specified AP.

- Run the ***logging server*** *ip-address* ***[udp-port*** *num****]*** command to configure the IP address of the system log server of a specified AP.

Command	**loggingon** **no loggingon**
Parameter Description	N/A
Defaults	The system logs are displayed by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Command	**logging server** *ip-address***[udp-port** *num***]** **no logging server** *ip-address*
Parameter Description	*ip-address*: indicates the IP address of the host that receives the log information. num: indicates the ID of the port on the host that receives the log information. This parameter is optional.
Defaults	N/A
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	You can configure at most five log server addresses. The log information will be sent simultaneously to all the configured log servers.

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

Disabling the Function of Displaying System Logs on Ruijie-AP1

Configuration Steps	● Enter the AP configuration mode. ● Disable the function of displaying system logs.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#no logging on`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  no logging on` `!`

Configuring the Log Server Address of Ruijie-AP1

Configuration Steps	● Enter the AP configuration mode. ● Set the log server address to 1.1.1.1.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#logging server 1.1.1.1`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  logging server 1.1.1.1` `!`

Common Errors

- N/A

1.4.13 Configuring the Daily Scheduled Restart Time for an AP

Configuration Effect

- If APs work too long, the load may be too heavy, affecting the network access quality of users. To prevent this problem, you can configure the daily scheduled restart time for an AP so that the network access quality of users can be ensured every day.

Notes

- N/A

Configuration Steps

- Optional. You can enable the daily scheduled restart function based on the AP load.
- Configure the daily scheduled restart time to prevent APs from working for a long time, enhancing availability of the network.

Command	**reload at***time* **no reload at**
Parameter Description	*time*: indicates the time when the AP is restarted every day. The time is expressed in the format of hh:mm:ss.
Defaults	The daily scheduled restart function of an AP is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to check the configurations.

Configuration Example

↘ Enabling Ruijie-AP1 to Restart at 1:00:00 Every Day

Configuration Steps	• Enable Ruijie-AP1 to restart at 1:00:00 every day. • Use the **no** form of the command to cancel the scheduled restart configuration.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#reload at 1:00:00` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ac)#no reload at`
Verification	Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  reload at 1:00:00` `!`

Common Errors

- N/A

1.4.14 Restoring Factory Settings of a Specified AP

Configuration Effect

- Restore factory settings of a specified AP.
- The configuration takes effect only on an online AP.

Notes

- This operation will cause offline and reset of the AP.

Configuration Steps

- Optional. You can restore factory settings of a specified AP according to requirements.
- Restoring AP factory settings is an instant behavior of an AP. This command can restore factory settings of the AP and will trigger reset of the AP.

Command	**factory-reset***ap-name*

Parameter Description	*ap-name*: indicates the name of an AP.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This operation will cause reset of the AP.

Verification

- After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings of the AP are restored.

Configuration Example

Restoring Factory Settings of the Online AP Ruijie-AP1

Configuration Steps	• Enter the AC configuration mode. • Restore factory settings of the online AP Ruijie-AP1.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#factory-reset Ruijie-AP1`
Verification	After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings (null settings) of the AP are restored.

Common Errors

- N/A

1.4.15 Resetting an AP

Configuration Effect

- Reset an online AP.
- Reset all online APs.

Notes

- N/A

Configuration Steps

- Optional. You can reset one or more APs according to requirements.
- If you configure AP reset on the AC, the corresponding AP will reset. You can configure reset of a specified AP or all online APs.

Command	**reset**{ **all** |**single** *ap-name*}

Parameter Description	**all**: indicates that all online APs are reset. **single *ap-name***: indicates that a specified AP is reset.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- After the configuration is completed, you can view the syslog record on the AC, indicating that the corresponding AP goes offline, and the AP will be reset.

Configuration Example

Resetting Ruijie-AP1

Configuration Steps	• Enter the AC configuration mode. • Reset Ruijie-AP1.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#` `Ruijie(config-ac)#reset Ruijie-AP1`
Verification	Check whether Ruijie-AP1 is reset, and whether the following syslog record indicating the offline event of the AP can be viewed on the AC.
AC	`%APMG-6-RX_CTRL_MSG: AP(AP_20#3F_S:001a.a912.3456) leave AC.`

Common Errors

- N/A

1.4.16 Configuring the AP Quantity Limit

Configuration Effect

- The number of online APs connected to the AP does not exceed the configured maximum number of APs supported by the AC.

Notes

- The weight of an AP varies according to the AP model. For example, the weight of one WALL-AP is 0.5 and two WALL-APs are treated as one AP. When APs are connected to an AC, the weighted number of APs is calculated based on the weight. This command and the license control the weighted number of APs, instead of the actual number of APs.

Configuration Steps

- Optional. You can configure the AP quantity limit within the capacity range according to requirements.

Command	**wtp-limit** *max-num*
Parameter Description	*max-num*: indicates the maximum number of APs that can be connected to an AC.
Defaults	By default, this number is equal to the number of APs supported by an AC.
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the maximum number of APs connected to an AC. This number cannot exceed the maximum number of APs supported by the AC or the maximum number of APs allowed by the license.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

Setting the Maximum Number of APs Connected to the AC to 512

Configuration Steps	• Enter the AC configuration mode. • Set the maximum number of APs connected to the AC to 512. • Use the **no** form of this command to restore the default setting.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#wtp-limit 512` `Ruijie(config)#ac-controller` `Ruijie(config-ac)#no wtp-limit`
Verification	Run the **show ac-config** command to check the configured maximum number of APs that can be connected to the AC.
AC	`Ruijie#show ac-config` `…` `max_wtp :512` `…`

Common Errors

- N/A

1.4.17 Configuring the AP Compliance Check

Configuration Effect

- The AP compliance check is also called AP access control based on the bound MAC address, or bind-ap-mac function. If AP compliance check is enabled, only APs that have offline configurations bound with their MAC addresses are allowed to associate with the AC.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP compliance check to allow only APs with specified MAC address to go online, thus implementing strict control on access of APs.
- When the AP compliance check is enabled, all online APs are automatically bound with MAC addresses. Therefore, it is recommended that this function be disabled during network deployment, and enabled after all APs within the plan go online.
- When the **bind-ap-mac** function is enabled, MAC addresses automatically bound with all online APs are converted to the formal MAC address binding, which is not automatically deleted when APs go offline.
- On the AC device, you can run the **ap-mac** *X.Y.Z* command in AP configuration mode to configure the MAC address binding of an individual AP configuration.

Command	**bind-ap-mac** **no bind-ap-mac**
Parameter Description	N/A
Defaults	The AP compliance check is disabled by default.
Command Mode	AC configuration mode
Usage Guide	This command is used to enable the AP compliance check.

Command	**ap-mac** *ap-mac-address* **no ap-mac**
Parameter Description	*ap-mac-address*: indicates the MAC address that is bound.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	The **ap-mac***ap-mac-address* command is applicable to offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online.

Verification

- Run the **show running** command to check whether the **bind-ap-mac** function is enabled.
- Run the **show ap-config running** command to check the MAC address binding information of AP configurations.

Configuration Example

Enabling the bind-ap-mac Function on an AC

Configuration Steps	● After all authorized APs go online, enter the AC configuration mode and run the **bind-ap-mac** command to enable the bind-ap-mac function.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#bind-ap-mac`
Verification	Run the **show running** command to check whether the bind-ap-mac function is enabled.
AC	`Ruijie#show running` `!` `ac-controller` `  bind-ap-mac` `!`

Common Errors

- N/A

1.4.18 Configuring AP Access Authentication

Configuration Effect

- AP access authentication can be implemented based on the serial number, password, or certificate.

Notes

- If you run the **ap-auth** { **serial** | **password** | **certificate** } **enable** command in AC configuration mode to enable the access authentication function, but do not run the **ap-auth** { **serial** *serial-string* |**password** *password* |**ac-cert** *ac-cert-name* |**ap-cert** *ap-cert-name* } command in AP configuration mode to configure related authentication parameters, AP access authentication will fail and the AP cannot go online.

Configuration Steps

- Optional.
- Run the **ap-auth serial-update** command to update the authentication serial numbers for all online APs.
- Run the **ap-auth enable** command in AC configuration mode to enable a specified type of AP access authentication.

- Run the **ap-auth** { **serial** *serial-string*|**password** *password* |**ac-cert** *ac-cert-name* |**ap-cert** *ap-cert-name* } command to configure the related AP access authentication parameters.

Command	**ap-auth serial-update**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	All online APs use the current AP serial numbers for authentication.

Command	**ap-auth** {**serial** |**password** |**certificate**} **enable**
Parameter Description	**serial**: indicates the authentication function based on the AP access serial number. **password**: indicates the authentication function based on the AP access password. **certificate**: indicates the authentication function based on the AP certificate.
Defaults	The authentication function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**ap-auth**{**serial** *serial-string*|**password** *password* |**ac-cert** *ac-cert-name*|**ap-cert** *ap-cert-name*}
Parameter Description	*serial-string*: indicates the AP access serial number. *password*: indicates the AP access password. *ac-cert-name*: indicates the AC certificate file name. *ap-cert-name*: indicates the AP certificate file name.
Defaults	This function is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The AP access authentication configurations take effect only when the AP makes an access attempt. If the AP is already online, the configurations take effect next time when the AP goes online. The **ap-auth serial** command cannot be used in all-AP configuration mode because the serial number varies according to the AP. The certificate file issued by the **ap-auth ap-cert** command will be stored as **cert.crt** on the AP, and the file name cannot be changed.

Verification

- Run the **show ap-config running** command to check whether the configuration is successful.

Configuration Example

↘ Configuring the AP Access Authentication Function Based on the Serial Number

Configuration Steps	● After all authorized APs go online, update the authentication serial numbers for all online APs. ● Enable the AP access authentication function based on the serial number. ● Configure the authentication serial number of a specified AP.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#ap-auth serial-update` `Ruijie(config)#ac-controller` `Ruijie(config-ac)#ap-auth serial enable` `Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#ap-auth serial G1GD10U000456`
Verification	Run the **show running** or **show ap-config running** command to check the AP access authentication configurations.
AC	`Ruijie(config)#show run` `!` `ac-controller` `  ap-auth serial enable` `!` `Ruijie(config)#show ap-config running Ruijie-AP1` `!` `ap-config Ruijie-AP1` `  ap-auth serial G1GD10U000456` `!`

↘ Updating the Access Authentication Certificate of an AP

Configuration Steps	● Update the access authentication certificate of an AP.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#ap-auth ap-cret ap1_cret.crt`
Verification	Run the **show ap-config running** command to check the name of the current AC. If the corresponding AP is online, the **ap1_cret.crt** file is updated to the AP instantly; otherwise, the file is updated to the AP after the AP goes online.
AC	`Ruijie(config)#show ap-config running Ruijie-AP1` `!`

	ap-config Ruijie-AP1 ap-auth ap-cret apl_cret.crt !

Common Errors

- N/A

1.4.19 Configuring the AP Priority

Configuration Effect

- By default, the AC allows the access of APs based on the sequence of AP association requests received by the AC. You can set the failover priorities of APs and enable the AC to support the failover priorities of APs so that the AC can allow the access of APs based on the AP priorities. The AP priority ranges from 1 to 4, where 1 is the lowest priority.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP priority function according to requirements and configure the priority of a specified AP.
- On the AC device, enter the AC configuration mode and run the **ap-priority** { **enable** | **disable** } command to enable or disable the AP priority function.
- On the AC device, enter the AP configuration mode and run the **priority** *priority-value* command to configure the priority of a specified AP.

Command	**ap-priority** { **enable**	**disable**}
Parameter Description	**enable**: enables the AP to support the failover priority. **disable**: disables the AP to support the failover priority.
Defaults	Disable
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**priority** *priority-value*
Parameter Description	priority-value: indicates the AP priority. The value ranges from 1 to 4, where 1 is the lowest priority.
Defaults	The default priority of an AP is 1. The priority can be set to a value from 1 to 4, where 1 is the lowest priority and 4 is the highest priority. You can run the **priority** command in AP configuration mode to configure the AP priority.

Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show ap-config running** command to check the configurations.

Configuration Example

Setting the Priority of Ruijie-AP1 to 2 and Enabling the AP Priority Function

Configuration Steps	• Enter the AP configuration mode. • Configure the AP priority. • Enter the AC configuration mode. • Enable the AP priority function.
AC	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#priority 2` `Ruijie(config)#ac-controller` `Ruijie(config-ac)#ap-priority enable`
Verification	Run the **show running** command to check whether the **ap-priority enable** command is configured in AC configuration mode. Run the **show ap-config running** command to check the AP configurations.
AC	`Ruijie(config)#show running` `!` `ac-controller` `  ap-priority enable` `!` `Ruijie#show ap-config running` `!` `ap-config Ruijie-AP1` `  priority 2` `!`

Common Errors

- N/A

1.4.20 Configuring the AC Cluster Function

Configuration Effect

- AC cluster is also called AC redundancy. With this function, multiple ACs with different priorities are designated for an AP. When the connection between the AP and a high-priority AC is down, the AP is connected to a low-priority AC (standby AC). When the connection with the high-priority AC is recovered, the AP disconnects the CAPWAP tunnel with the low-priority AC, and sets up a CAPWAP tunnel with the high-priority AC again.
- On the one hand, the AC cluster function enhances reliability of the AC cluster. On the other hand, this function controls the home AC of APs in stable conditions based on the priority to facilitate AP management.

Notes

- For a specified AP, the same priority must be configured for this AP on each AC that belongs to the cluster. For example, on AC1, AC2 is configured as the primary AC for AP1, and AC1 is configured as the secondary AC for AP1. On AC2, AC1 is configured as the primary AC for AP1, and AC2 is configured as the secondary AC for AP1. That is, on both AC1 and AC2, the peer AC is configured as the high-priority AC for AP1. In this way, an endless loop is formed because the AP keeps switching between tunnels with two ACs.
- The redundancy AC configuration supports both the ap-config ap-name and ap-config all configuration modes. The redundancy AC configuration made in ap-config ap-name configuration mode takes precedence over that made in ap-config all configuration mode.
- Except the **primary-base** command, commands of other priorities do not support switchback to prevent network interruption caused by the switchback. The administrator can re-configure the priorities for a manual switchover, or configure the **switch-back** parameter for an automatic switchback.

Configuration Steps

- Optional. The redundancy AC configuration does not exist on an AP by default. You can configure redundancy ACs with different priorities for an AP based on the number of ACs deployed on the wireless network.
- Run the **primary-base** *ac-name* { *ip-address* | *ipv6-address* } command to configure the primary AC for a specified AP.
- Run the **secondary-base** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the secondary AC for a specified AP.
- Run the **tertiary-base***ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the tertiary AC for a specified AP.
- Run the **backup-controller-primary***ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the fourthAC for a specified AP.
- Run the **backup-controller-secondary***ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the fifthAC for a specified AP.
- Run the **backup-controller-tertiary***ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the sixthAC for a specified AP.

Command	**primary-base***ac-name* { *ip-address*	*ipv6-address* }

	no primary-base
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the primary AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the primary AC. The format is X;Y::Z.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**secondary-base***ac-name* {*ip-address* | *ipv6-address* }[**switch-back**] **no secondary-base**
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**tertiary-base***ac-name* {*ip-address* | *ipv6-address*}[**switch-back**] **no tertiary-base**
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-primary***ac-name* {*ip-address* | *ipv6-address*}[**switch-back**] **no backup-controller-primary**
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: indicates the switchback function. Switchback is disabled by default.
Defaults	N/A

Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-secondary***ac-name* { *ip-address* | *ipv6-address*}[**switch-back**] **no backup-controller-secondary**
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-tertiary***ac-name* { *ip-address* | *ipv6-address* }[**switch-back**] **no backup-controller-tertiary**
Parameter Description	*ac-name*: indicates the name of the AC to be configured. *ip-address*: indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

Configuring Ruijie-AC1 as the Primary AC of Ruijie-AP1, and Ruijie-AC2 as the Secondary AC

Configuration Steps	• Enter the AP configuration mode. • Configure the primary AC and secondary AC of the AP.
Ruijie-AC1	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#primary-base Ruijie-AC1 5.5.5.5` `Ruijie(config-ap)#secondary-base Ruijie-AC2 6.6.6.6`

Ruijie-AC2	`Ruijie(config)#ap-config Ruijie-AP1` `Ruijie(config-ap)#primary-base Ruijie-AC1 5.5.5.5` `Ruijie(config-ap)#secondary-base Ruijie-AC2 6.6.6.6`
Verification	Run the **show ap-config running** command to check the AP configurations.
Ruijie-AC1	`Ruijie#show ap-config running` `!` `ap-config Ruijie-AP1` `  primary-base Ruijie-AC1 5.5.5.5` `secondary-base Ruijie-AC2 6.6.6.6` `!`
Ruijie-AC2	`Ruijie#show ap-config running` `!` `ap-config Ruijie-AP1` `  primary-base Ruijie-AC1 5.5.5.5` `secondary-base Ruijie-AC2 6.6.6.6` `!`

Common Errors

- N/A

1.4.21 Configuring the AC Hot Backup Function

Configuration Effect

- Set up the hot backup connection to ensure that the AP can set up two CAPWAP tunnels.

Notes

- N/A

Configuration Steps

- Optional. If an AP does not use the hot backup address of the AC to set up a tunnel, the AC address of the first tunnel must be specified. When IPv6must be used to set up the second channel, the IPv6 hot backup tunnel function must be enabled.
- Run the **peer-ip** command to configure the IP address for setting up a CAPWAP tunnel with the hot backup neighbor. This IP address will be pushed to the AP device, and the AP device will set up the second CAPWAP tunnel with the hot

backup neighbor based on the peer-ip address. If the AP does not use the default hot backup address of the AC to set up a tunnel, you need to configure the peer-ip address.

- Run the **peer-ipv6** command to configure the IPv6 address for setting up a CAPWAP tunnel with the hot backup neighbor. This IPv6 address will be pushed to the AP device, and the AP device will set up the second CAPWAP IPv6 tunnel with the hot backup neighbor based on the peer-ipv6 address. When an AP and an AC use the IPv6 address to set up a tunnel, you need to configure the peer-ipv6 address to set up the second CAPWAP IPv6 tunnel because currently IPv6 cannot be used for setting a hot backup connection between ACs.
- After the **peer-ipv6 enable** command is executed, the AP device sets up the second CAPWAP IPv6 tunnel with the hot backup neighbor. To set up a CAPWAP IPv6 tunnel between an AP and an AC, you must enable peer-ipv6so that the second CAPWAP IPv6 tunnel can be set up between the AP and the AC.
- Run the **ap-group** command to bind an AP group with the hot backup instance. After the AP group is bound with the hot backup instance, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.

Command	**peer-ip***ipv4-address*
Parameter Description	*ipv4-address*: indicates the IP address used by the hot backup neighbor to set up a CAPWAP tunnel.
Defaults	Source address used by CAPWAP
Command Mode	Hot backup instance mode
Usage Guide	In the non-NAT environment, use the default setting, that is, the source address used by CAPWAP. In the NAT environment, configure the IPv6 address based on the environment where the AC and AP are located. When the AC is located inside the NAT, its address is a private network address, which is not accessible by the AP. Therefore, the AP must be notified of the configured public network address. ● If both the AP and the AC are within the NAT internal network, use the default setting. ● If the AP is in the NAT external network, use the IP address configured by the user as the peer AC address.

Command	**peer-ipv6***ipv6-address*
Parameter Description	*ipv6-address*: indicates the IPv6 address used by the hot backup neighbor to set up a CAPWAP tunnel.
Defaults	Source address used by CAPWAP
Command Mode	Hot backup instance mode
Usage Guide	In the non-NAT environment, use the default setting, that is, the source address used by CAPWAP. In the NAT environment, configure the IPv6 address based on the environment where the AC and AP are located. When the AC is located inside the NAT, its address is a private network address, which is not accessible by the AP. Therefore, the AP must be notified of the configured public network address. ● If both the AP and the AC are within the NAT internal network, use the default setting.

	● If the AP is in the NAT external network, use the IP address configured by the user as the peer AC address. You need to run the **peer-ipv6 enable** command to enable the function of using CAPWAP to set up the dual IPv6 hot backup tunnels.

Command	**peer-ipv6 enable**
Parameter Description	N/A
Defaults	Disable
Command Mode	Hot backup instance mode
Usage Guide	The peer-ipv6must be enabled when CAPWAP is used to set up an IPv6 tunnel between the AP and a hot backup AC so that the AP can use CAPWAP to set up an IPv6 tunnel with another hot backup AC.

Command	**ap-group** *ap-group*
Parameter Description	*ap-group*: indicates the name of an AP group.
Defaults	N/A
Command Mode	Hot backup instance mode
Usage Guide	After the AP group is bound with the hot backup instance, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.

Verification

● Run the **show running** command to check the configurations.

Configuration Example

For details about the AC hot backup deployment solution, see "WLAN Hot Backup."

Enabling the AC to Use the Public Network Address as the AC Address

Configuration Steps	● Configure the hot backup address and enter the hot backup configuration mode. ● Configure the hot backup instance. ● In the hot backup instance configuration mode, configure the peer IP address.
AC	`Ruijie(config-hotbackup)# context 10` `Ruijie(config-hotbackup-ctx)# peer-ip 1.1.1.1`
Verification	Run the **show running** command to check the configurations.
AC	`Ruijie(config)#show running`

	wlan hot-backup 1.1.1.1 ! context 10 peer-ip 1.1.1.1

Common Errors

- N/A

1.4.22 Creating a WLAN

Configuration Effect

- You can create multiple WLANs on an AC and enter the configuration mode of a specified WLAN to configure related functions and properties of the WLAN according to the actual network requirements.
- The WLAN service template that is generated based on the following configurations can take effect only after the WLAN is deployed on a specified AP group. Wireless users can access related APs to access the WLAN.
- On the wireless network, you can divide the network into multiple WLAN subnets by creating WLANs. In addition, you can configure the functions and properties of a specified WLAN in WLAN configuration mode to provide different network services for wireless users.
- When creating a WLAN, you must associate the WLAN with an SSID, which is the name of a network service zone. One SSID can be mapped to one or multiple WLANs.

Notes

- N/A

Configuration Steps

- Optional. No WLAN is configured by default. You must create a WLAN before deploying the WLAN.
- Run the **wlan-config** command to create a WLAN, and use the **no** form of the command to delete the WLAN.

Command	**wlan-config***wlan-id* [*profile –string*][*ssid-string*] **no wlan-config***wlan-id*
Parameter Description	*wlan-id*: indicates the ID of a WLAN. The value ranges from 1 to 4094. *profile -string*: indicates the profile of the WLAN. This parameter is optional. The maximum length is 32 bytes. *ssid-string*: indicates the SSID. The maximum length is 32 bytes. When creating a WLAN, you must specify the SSID associated with the WLAN. Use the **no** form of the command to delete a specified WLAN.
Defaults	No WLAN is created by default.
Command Mode	Global configuration mode

Usage Guide	One SSID can be mapped to one or multiple WLANs, but one WLAN can be associated with only one SSID.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

↘ Creating a WLAN

Configuration Steps	● Create WLAN 1. The SSID of WLAN 1 is ruijie-wireless.
AC	`Ruijie(config)#wlan-config 1 ruijie-wireless` `Ruijie(config-wlan)#`
Verification	Run the **show running** command to check the WLAN configurations.
AC	`Ruijie#show running` `!` `wlan-config 1 ruijie-wireless` `!`

Common Errors

- N/A

1.4.23 Deploying a WLAN

Configuration Effect

- The WLAN configuration takes effect only after the WLAN is deployed on a specified AP group. Wireless users can access the WLAN through the related APs. Run the **interface-mapping** command in AP group configuration mode to deploy the WLAN on a specified AP group. This command also configures the mapping between the WLAN and the VLANs or VLAN group of the wired network.

Notes

- Assume that the WLAN forwarding mode is local forwarding. In this case, if the vlan-id assigned to a STA in vlan-id or vlan-group mode configured by this **interface-mapping** command is the same as the vlan-id specified by the **ap-vlan** command, the real VLAN of the STA will be determined by the access switch of the AP, instead of the VLAN configured by the **interface-mapping** command or the VLAN assigned in vlan-group mode. In particular, the default vlan-id of the ap-vlan is 1. If the ap-vlan is not configured and the vlan-id configured in the **interface-mapping** command is 1, the VLAN of the STA in local forwarding mode is determined by the access switch.

Configuration Steps

- Optional. You can run the **interface-mapping** command in AP group configuration mode to configure a WLAN and deploy the WLAN on all APs in the AP group.
- On the AC device, enter the AP configuration mode and run the **interface-mapping** command for configuration.

Command	**interface-mapping***wlan-id*{*vlan-id* I **group***vlan-group-id*}[**radio**{*radio-id*	[*802.11b*	*802.11a*]}] [**ap-wlan-id***ap-wlan-id*]
Parameter Description	*wlan-id*: indicates the ID of the specified WLAN. This WLAN must have been created. The WLAN ID ranges from 1 to 4094. *vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. vlan-group-id: indicates the ID of the specified VLAN group. The VLAN group ID ranges from 1 to 128. r*adio-id*: indicates the ID of the radio of a specified AP. If radio-id is not specified, the mapping is applied to all radios of all APs in the AP group. The radio ID ranges from 1 to 96. *802.11b*: indicates that the mapping is applied to all 2.4 GHz radios of all APs in the AP group. *802.11a*: indicates that the mapping is applied to all 5.8 GHz radios of all APs in the AP group. *ap-wlan-id*: specifies the wlan-id that is used on the AP through interface-mapping. The value ranges from 1 to 64.
Defaults	By default, the WLAN is not deployed on any AP.
Command Mode	AP group configuration mode
Usage Guide	If the **ap-wlan-id** parameter is not specified, the mapping automatically selects and uses an idle ap-wlan-id.

Verification

- Run the **show running** command to check the AP group configurations.

Configuration Example

Configuring a WLAN and Deploying the WLAN on a Specified AP Group

Configuration Steps	Ruijie-AP1 belongs to the AP group APG-1. Create a WLAN, and deploy the WLAN on Ruijie-AP1. - Create WLAN 1. The SSID of WLAN 1 is ruijie-wireless. - Create VLAN 1. - Configure the WLAN-VLAN mapping in AP group configuration mode.
AC	`Ruijie(config)#wlan-config 1 ruijie-wireless` `Ruijie(config-wlan)#exit` `Ruijie(config)#vlan 1` `Ruijie(config-vlan)#exit` `Ruijie(config)#ap-group APG-1`

	`Ruijie(config-ap-group)#interface-mapping 1 1`
Verification	Run the **show running** command to check the AP group configurations.
	`Ruijie#show running` `!` `wlan-config 1 ruijie-wireless` `!` `!` `ap-group APG-1` `  interface-mapping 1 1` `!`

Common Errors

- N/A

1.4.24 Enabling or Disabling WLAN SSID Broadcasting

Configuration Effect

- On the WLAN, the AP periodically broadcasts the SSID information to notify other entities of the existence of the wireless network. Wireless users use the wireless network interface cards (NICs) to search SSIDs and detect the wireless network. The SSID broadcasting function can be enabled to prevent the wireless network from being searched and connected by unauthorized users based on the SSID.

Notes

- N/A

Configuration Steps

- Optional. WLAN SSID broadcasting is enabled by default. If the WLAN SSID should be hidden to prevent the wireless network from being searched and connected by unauthorized users based on the SSID, you can disable the WLAN SSID broadcasting function.
- On the AC device, enter the WLAN configuration mode and run the **enable-broad-ssid** command for configuration.

Command	**enable-broad-ssid** **no enable-broad-ssid**
Parameter Description	N/A
Defaults	WLAN SSID broadcasting is enabled by default.
Command Mode	WLAN configuration mode

Usage Guide	WLAN SSID broadcasting is enabled by default. You can use the **no** form of the command to disable this function. If the SSID broadcasting configuration of the WLAN changes, users associated with the WLAN will go offline.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Disabling SSID Broadcasting of WLAN 1

Configuration Steps	• Enter the WLAN configuration mode. • Disable SSID broadcasting.
AC	`Ruijie(config)#wlan-config 1` `Ruijie(config-wlan)#no enable-broad-ssid`
Verification	Run the **show running** command to check the WLAN configurations.
AC	`Ruijie#show running` `!` `wlan-config 1 ruijie-wireless` `  no enable-broad-ssid` `!`

Common Errors

- N/A

1.4.25 Configuring the NAS ID of a WLAN User

Configuration Effect

- On the WLAN, the NAS IDs of WLAN users identify different hot spot areas. By default, the NAS ID of a WLAN user is a null string.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC device, enter the WLAN configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *wlan-nas-id*

	no nas-id
Parameter Description	N/A
Defaults	Null string
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

Configuring the NAS ID of a WLAN User

Configuration Steps	• Enter the WLAN configuration mode. • Configure the NAS ID of a WLAN user.
AC	`Ruijie(config)#wlan-config 1` `Ruijie(config-wlan)#nas-id0000059159100460`
Verification	Run the **show running** command to check the WLAN configurations.
AC	`Ruijie#show running` `!` `wlan-config 1 ruijie-wireless` `nas-id0000059159100460` `!`

Common Errors

- N/A

1.4.26 Configuring the Fit or Fat AP Mode

Configuration Effect

- On the AC device, run the **switch2fat** command in AC configuration mode to switch the mode of an online AP to the fat AP mode.
- On the AC device, run the **ap-mode** command in global configuration mode to switch between the fit AP mode and the fat AP mode.

Notes

- If the **switch2fat** command is executed on the AC in AP configuration mode to switch the mode of an online AP to the fat AP mode, the AP will be disconnected from the AC. After that, you cannot configure the AP on the AC.

Configuration Steps

- Optional. For an AC, an online AP definitely works in fit AP mode. You can run the **switch2fat** command if you need to switch the mode of the AP to the fat AP mode.
- On the AC device, run the **switch2fat** command in AC configuration mode to switch the mode of an online AP to the fat AP mode.
- On the AC device, run the **ap-mode** command in global configuration mode to switch between the fit AP mode and the fat AP mode.

Command	**switch2fat** *ap-name*
Parameter Description	*ap-name*: indicates the name of a specified AP.
Defaults	By default, all fit APs are controlled by the associated AC. A fit AP can be switched to a fat AP to implement self-control.
Command Mode	AC configuration mode
Usage Guide	This command takes effect only on an online AP.

Command	**ap-mode**{ **fit** | **fat**[**dhcp**]}
Parameter Description	**fit**: indicates that the AP mode is switched to the fit AP mode. **fat:** indicates that the AP mode is switched to the fat AP mode. **dhcp**: If the **ap-mode fat** command contains this parameter, the AP obtains the IP address through DHCP by default after the AP mode is switched to the fat AP mode; otherwise, the AP uses the static IP address by default after the AP mode is switched to the fat AP mode.
Defaults	N/A
Command Mode	AP global configuration mode
Usage Guide	After the AP mode is switched between the fit and fat AP modes, the AP must be restarted to ensure the configuration consistency. For WALL-APs supplied by Ruijie Networks, when the fat AP mode is used, the default IP address of the rear wired network interface (connected to the PoE switching device) is 192.168.110.1/255.255.255.0, and the default IP address of the front wired network interface (Ethernet interface) is 192.168.111.1/255.255.255.0. If **ap-mode fat dhcp** is configured, when the AP mode is switched to the fat AP mode, the IP address is obtained through DHCP by default. After the AP is restarted, if related configuration is not available, the IP address is still obtained through DHCP by default. In addition, the following two issues should

	also be noted: 1.If **ap-mode fat dhcp** is configured for the WALL-AP, only the IP address of the rear wired network interface is obtained through DHCP, and the front wired network interface uses the static IP address by default. 2.In fat AP mode, the **ap-mode fat dhcp** and **ap-mode fat** commands cannot be mutually switched, and must be switched to the fit AP mode first. In fit mode, the default password for the user EXEC mode is **ruijie** and that for the privileged EXEC mode is **apdebug**. In fat/fat dhcp/macc mode, the default password for user EXEC mode is **admin** and that for the privileged EXEC mode is empty.

Verification

- On the AP, run the **show ap-mode** command to check the current mode of the AP.

Configuration Example

Switching the Mode of the Online AP Ruijie-AP1 to the Fat AP Mode on the AC

Configuration Steps	• Enter the AC configuration mode. • Run the **switch2fat** command.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#switch2fat Ruijie-AP1`
Verification	On the AP, run the **show ap-mode** command to check the current mode of the AP.
AP	`Ruijie#show ap-mode` `current mode: fat`

Common Errors

- N/A

1.4.27 Configuring the WLAN SSID

Configuration Effect

- Configure a new SSID for the WLAN. If this WLAN has been deployed, all users associated with this WLAN will go offline.
- Configure the coded character set for the SSID. If the WLAN is deployed, all users of this WLAN will go offline.

Notes

- N/A

Configuration Steps

- Optional.

- On the AC device, enter the WLAN configuration mode and run the **ssid** command to configure the new SSID.

Command	**ssid** *ssid-string*
Parameter Description	N/A
Defaults	N/A
Command Mode	WLAN configuration mode
Usage Guide	N/A

- On the AC device, enter the WLAN configuration mode and run the **ssid-code** command to configure the coded character set for the SSID.

Command	**ssid-code** { **gbk** | **utf-8** }
Parameter Description	**gbk**: Configures gbk. **utf-8**: Configures utf-8.
Defaults	N/A
Command Mode	WLAN configuration mode
Usage Guide	If the WLAN is deployed, all users of this WLAN will go offline.

Verification

- Run the **show running** command to check the WLAN configurations.

Configuration Example

↘ Configuring a New SSID "ruijie" for WLAN 1

Configuration Steps	• Enter the WLAN configuration mode. • Configure a new SSID "ruijie".
AC	`Ruijie(config)#wlan-config 1` `Ruijie(config-wlan)#ssid ruijie`
Verification	Run the **show running** command to check the WLAN configurations.
AC	`Ruijie#show running` `!` `wlan-config 1 ruijie` `!`

Common Errors

- N/A

1.4.28 Configuring the AP Backup Function

Configuration Effect

- If the active AP in an AP backup group is faulty and disconnected, other standby APs in the group receive the WLAN configuration of the active AP and transmit radio signals of the active AP.

Notes

- In an AP backup group, if the active AP is not selected, the AP backup function does not take effect.

Configuration Steps

Configuring an AP Backup Group

- Optional. Create an AP backup group when the wireless network of an AP needs to be backed up.
- In AC configuration mode, run the **ap-backup group** command to create an AP backup group.

Command	**ap-backup group** *backup-group*
Parameter Description	*backup-group*: indicates the name of the AP backup group.
Defaults	By default, if only the AP backup group named "default" exists on the AC, the backup function of this group does not take effect.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an AP Backup Group

- Optional. When the wireless network of an AP must be backed up by other APs, add the standby APs and the AP to be backed up to the AP backup group, and select the AP to be backed up as the active AP.
- In AP configuration mode, run the **ap-backup-group** command to add the AP to the AP backup group. When adding an AP to an AP backup group, you can specify whether the AP is the active AP.

Command	**ap-backup-group** *backup-group***[master]**
Parameter Description	*backup-group*: indicates the name of the AP backup group.
Defaults	By default, the AP is not added to the default group, and the backup function of the backup group does not take effect.
Command Mode	AP configuration mode
Usage Guide	This command does not support the ap-config all mode. The keyword **master** is optional. If the command contains this keyword, the AP is designated as the active AP of the group; otherwise, the AP is the standby AP. An AP backup group can have multiple standby APs but only one active AP.

	When the AP backup group starts to work, that is, the standby APs have inherited WLAN signals from the active AP, note that the following four operations change the WLAN configurations of the standby APs that should take effect, and the inherited WLAN signals will take effect again: 1. Modify the WLAN configurations of the AP group to which the standby APs belong. 2. Modify the WLAN configurations of the AP group to which the active AP belongs. 3. Change the AP group of the standby APs. 4. Change the AP group of the active AP. If online users already exist, these users will go offline.

Verification

- Run the **show ap-config running** and **show ac-config ap-backup-group** commands to check the configurations.

Configuration Example

Creating an AP Backup Group Named "APBACK-APG-1"

Configuration Steps	● In AC configuration mode, run the **ap-backup group** command to create an AP backup group.
AC	`Ruijie(ac-config)#ap-backup group APBACK-APG-1`
Verification	● Run the **show ac-config ap-backup-group** command to check the configurations.
AC	`Ruijie#show ac-config ap-backup-group` `Cnt Group-Name Master-AP cntStandby-AP cnt Master-AP-Name Working` `------ ---------- ---------- ---------- ---------- -------` `1 APBACK-APG-1 1 2 AP4210-1 false`

Adding ap4210-1 to the AP Backup Group Named "APBACK-APG-1", and Configuring this AP as the Active AP of the Group

Configuration Steps	● In AP configuration mode, run the **backup-group** command to add the AP to the AP backup group.
AC	`Ruijie(ap-config)#ap-backup-group APBACK-APG-1 master`
Verification	● Run the **show ac-config ap-backup-group** command to check the configurations.
AC	`Ruijie#show ac-config ap-backup-groupAPBACK-APG-1` `Cnt Ap-Name Ap-Mac Online Is-Master Inherit-Wlan Cnt`

	------- ---------------------- ------------------- ------- ------------ -- ---------- 1 AP4210-1 8832.0000.1111 true Yes 0

Common Errors

- N/A

1.4.29 Configuring AC Virtualization Function

Configuration Effect

- After an administrator logs in to the web management page, the administrator can only check and configure authorized WLANs, AP groups, and APs (STAs).

Notes

- N/A

Configuration Steps

Configuring AC Virtualization Function

- Optional. When multiple administrators are required in a wireless environment to manage different wireless networks and APs, enable the AC virtualization function.
- Run the **permit enable** command in AC configuration mode to enable the AC virtualization function.
- Run the **master-group** command in global configuration mode to create a role and enter the role configuration mode.
- Run the **master-group** command in AP configuration mode to assign an AP to a specific role.
- Run the **master-group** command in AP group configuration mode to assign an AP group to a specific role.
- Run the **master-group** command in WLAN configuration mode to assign a WLAN to a specific role.
- Run the **webmaster** command in role configuration mode to add/delete an administrator.

Command	**permit enable**
Parameter Description	N/A
Defaults	The AC virtualization function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**master-group** *master-group-name*
Parameter Description	*master-group-name*: Indicates the role name.

Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	When the **no** form of this command is used to delete a role, APs, AP groups, and WLANs assigned to the role are restored to the unassigned state and the administrator of this role is restored to the default role-free state.

Command	**master-group** *master-group-name*
Parameter Description	*master-group-name*: Indicates the role name.
Defaults	N/A
Command Mode	AP/AP group/WLAN configuration mode
Usage Guide	After a role is deleted, APs, AP groups, and WLANs assigned to the role are restored to the default unassigned state.

Command	**webmaster** *webmaster-name*
Parameter Description	*webmaster-name*: Indicates the administrator name.
Defaults	N/A
Command Mode	Role configuration mode
Usage Guide	When a role is deleted, the administrator of the role is restored to the default role-free state.

Verification

- Run the **show running-config** and **show ap-config running** commands to display configurations.

Configuration Example

↘ Enabling AC virtualization function

Configuration Steps	● Run the **permit enable** command in AC configuration mode to enable the AC virtualization function.
AC	`Ruijie(ac-config)# permit enable`
Verification	● Run the **show running-config** command to display configurations.
AC	`Ruijie# show running-config | begin ac-controller` `ac-controller` ` permit enable`

	ac-name Ruijie country CN

Creating Role test-group and Adding Administrator test-admin-1 for the Role

Configuration Steps	● Run the **master-group** command in global configuration mode to create the role (test-group) and enter the role configuration mode. ● Run the **webmaster** command in role configuration mode to add the administrator (test-admin-1).
AC	Ruijie(config)# master-group test-group Ruijie(config-master-group)# webmaster test-admin-1
Verification	● Run the **show running-config** command to display configurations.
AC	Ruijie# show running-config | begin master-group master-group test-group webmaster test-admin-1

Assigning AP (ap-1), AP Group (apg-1), and WLAN (1) to Role test-group

Configuration Steps	● Run the **master-group** command in AP configuration mode to assign the AP (ap-1) to the role (test-group). ● Run the **master-group** command in AP group configuration mode to assign the AP group (apg-1) to the role (test-group). ● Run the **master-group** command in WLAN configuration mode to assign the WLAN (1) to the role (test-group).
AC	Ruijie(config)# ap-config ap-1 Ruijie(config-ap)# master-group test-group Ruijie(config-ap)# exit Ruijie(config)# ap-group apg-1 Ruijie(config-group)# master-group test-group Ruijie(config-group)# exit Ruijie(config)# wlan-config 1 Ruijie(config-wlan)# master-group test-group
Verification	● Run the **show running-config** and **show ap-config running** commands to display configurations.
AC	Ruijie# show running-config | begin wlan-config 1 wlan-config 1 Ruijie master-group test-group ! Ruijie# show running-config | begin ap-group apg-1

	ap-group apg-1 master-group test-group ! Ruijie# show ap-config running | begin ap-config ap-1 ap-config ap-1 master-group test-group !

Common Errors

- N/A

1.4.30 Configuring the AP Virtualization Function

Configuration Effect

- Multiple ACs can assign their own WLANs to the same AP, and the STAs connect to the virtual APs served by corresponding ACs.

Notes

- ACs cannot send the same signal.

Configuration Steps

Configuring an AP Virtualization Template

- Optional. Configure an AP virtualization template when multiple ACs need to manage the same AP.
- In global configuration mode, run the **virtual-ap** command to create an AP virtualization template.

Command	**virtual-ap** *sub-ap-name*
Parameter Description	*sub-ap-name*: Indicates the name of an AP virtualization template.
Defaults	No AP virtualization template is created by default.
Command Mode	AC global configuration mode
Usage Guide	N/A

Configuring the IP Address of the AC to Which a Virtual AP is to Connect

- Optional. If the IP address of the AC to which a virtual AP is to connect is not configured, the virtual AP created on the AP using the AP virtualization template cannot connect to the AC.

Command	**ac-ip** *ip*
Parameter Description	*ip*: Indicates the IPv4 address of the AC to which a virtual AP is to connect.
Defaults	The virtual APs created on the AP using the AP virtualization template cannot connect to ACs by default.

Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. The AP disconnects all tunnels and reconnects them each time the configurations are changed. The configured IP address cannot be the IP address of the active AC, and can only be the IP address of the AC to be connected and the address of the loopback 0 interface or the CAPWAP control IP address if any.

Configuring the Number of WLANs Supported by a Virtual AP

- Optional. If the number of WLANs supported by a virtual AP is not configured, it is calculated as follows:
  (Total number of WLANs supported by the AP – Number of WLANs configured for virtual APs)/Number of virtual APs with the number of supported WLANs not configured

Command	**wlan-capacity** *wlan-cap*
Parameter Description	*wlan-cap*: Indicates the number of WLANs supported by a virtual AP.
Defaults	The number of WLANs supported by a virtual AP is not configured by default.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, if the remaining number of WLANs is 0, the virtual AP cannot send wireless signals. The AP disconnects all tunnels and reconnects them each time the configurations are changed.

Configuring the Number of STAs Supported by a Virtual AP

- Optional. If the number of STAs supported by a virtual AP is not configured, it is calculated as follows:
  (Total number of STAs supported by the AP – Number of STAs configured for virtual APs)/Number of virtual APs with the number of supported STAs not configured

Command	**sta-capacity** *sta-cap*
Parameter Description	*sta-cap*: Indicates the number of STAs supported by a virtual AP.
Defaults	The number of STAs supported by a virtual AP is not configured by default.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, if the remaining number of STAs is 0, the virtual AP cannot send wireless signals.

	The AP disconnects all tunnels and reconnects them each time the configurations are changed.

Configuring the Uplink Interface Used by a Virtual AP

- Optional. If the uplink interface used by a virtual AP is not configured, the virtual AP uses the uplink interface used by the active AC.

Command	**link-interface** { *other* | *num}*
Parameter Description	*other*: Indicates that a virtual AP uses an uplink interface different from that used by the active AC. This parameter is specified when there are two uplink interfaces and virtual AP and active AC use them for connection. *num*: Indicates the number of uplink interface used by a virtual AP.
Defaults	A virtual AP uses the uplink interface used by the active AC by default.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, a virtual AP uses the uplink interface used by the active AC to establish a CAPWAP connection. The **other** parameter is configured only when there are two uplink interfaces and the virtual AP and active AC use them for connection. Otherwise, the virtual AP cannot establish a CAPWAP connection to the corresponding AC. If the configured uplink interface number does not exist, the virtual AP cannot establish a connection to the corresponding AC. The AP disconnects all tunnels and reconnects them each time the configurations are changed. If multiple uplink interfaces exist and the **other** or **num** parameter is configured after the aggregation function is configured, the virtual AP cannot establish a CAPWAP connection to the corresponding AC.

Configuring Virtual APs for an AP

- Optional. If virtual APs are not configured for an AP, the AP does not create virtual APs.

Command	**virtual-ap** *sub-ap-name* {**id** *num}*
Parameter Description	*sub-ap-name*: Indicates the name of an AP virtualization template. *num*: (Optional) Indicates the number of a virtual AP on the AP, which starts from 1 by default.
Defaults	An AP does not create virtual APs by default.
Command Mode	AP, AP group, and all-AP configuration modes
Usage Guide	This command is configured in AP, AP group, and all-AP configuration modes.

	In a configuration mode, multiple virtual APs can be configured but the virtual APs cannot have the same AC IP address except the default one. The AP disconnects all tunnels and reconnects them each time the configurations are changed. Configurations of the **virtual-ap** command are delivered based on the following priority sequence: Configurations in AP configuration mode > Configurations in AP group configuration mode > Configurations in all-AP configuration mode.

Configuring the Duration for a Virtual AP to Continue Service Provision After the Connection Between the AP and Active AC is Down

- Optional. If the duration for a virtual AP to continue service provision after interruption of the connection between the AP and active AC is not configured, the virtual AP continues to provide services for one day.

Command	**ap-idle-timeout** *num*
Parameter Description	*num*: Indicates the duration (in the unit of day) for a virtual AP to continue service provision after he connection between the AP and active AC is down. The value ranges from **0** to **14**.
Defaults	A virtual AP continues to provide services for one day by default after the connection between the AP and active AC is down.
Command Mode	AP, AP group, and all-AP configuration modes
Usage Guide	This command is configured in AP, AP group, and all-AP configuration modes. If the **num** parameter is set to **0** to prevent tunnel instability, the tunnel between the virtual AP and corresponding AC is not torn down immediately but retained for two minutes. After an AP disconnects from the active AC and the time specified in **ap-idle-timeout** has not expired, a virtual AP no longer connects to an AC if the tunnel between the virtual AP and corresponding AC is disconnected, and connects to the AC again only when the connection between the AP and active AC is re-established.

Verification

- Run the **show running** command to display configurations.

Configuration Example

Creating an AP Virtualization Template Named VAP-1

Configuration Steps	Run the **virtual-ap** command in AC global configuration mode to create the AP virtualization template named VAP-1.
AC	`Ruijie(config)#virtual-ap VAP-1` `Ruijie(config-virtual-ap)# wlan-capacity 6` `Ruijie(config-virtual-ap)# sta-capacity 6` `Ruijie(config-virtual-ap)# ac-ip 1.1.1.1`

	Ruijie(config-virtual-ap)# link-interface 2
Verification	● Run the **show running-config** command to display configurations.
AC	Ruijie#show running-config Building configuration... Current configuration: 6069 bytes version AC_RGOS 11.1(5)B00, Release(04150906) ! virtual-ap VAP-1 ac-ip 1.1.1.1 wlan-capacity 6 sta-capacity 16 link-interface 2 !

↘ Applying AP Virtualization Template VAP-1 to AP1

Configuration Steps	● Run the **virtual-ap** command in AP configuration mode, configuration mode of the AP group in which AP1 resides, or all-AP configuration mode.
AC	Ruijie(config)#ap-config AP1 You are going to config AP(AP1), which is not online now. Ruijie(config-ap)#virtual-ap VAP-1 Ruijie(config-ap)#
Verification	● Run the **show ap-config running** command to display configurations.
AC	Ruijie(config-ap)#show ap-c running ! ap-config AP1 virtual-ap VAP-1 id 1 !

Common Errors

- N/A

1.4.31 Configuring the Default SSID

Configuration Effect

- When a fit AP starts or the CAPWAP tunnel of the AP is disconnected, the AP releases a 2.4G unencrypted SSID signal. When the CAPWAP tunnel is set up, the SSID is disabled.

Notes

- If RIPT is configured and the tunnel is torn down, signals are not sent.
- When the AP is restarted, the configurations will be saved.

Configuration Steps

- Optional.
- On the AC, run the **offline-ssid** command in AP, AP group, or all-AP configuration mode to specify the SSID signal of the AP.

Command	**offline-ssid** *ssid* **[hide]** **no offline-ssid**
Parameter Description	*ssid*: Indicates the SSID signal broadcasted when the AP is started or the tunnel is torn down. **hide**: Indicates that no SSID signal is broadcasted.
Defaults	No SSID is configured by default.
Command Mode	AP configuration mode AP group configuration mode All-AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show ap-config running** command to display configurations.

Configuration Example

↘ Configuring the Default SSID of AP1 to my-def-ssid

- Configure the default SSID of the default AP group to my-group-ssid.

Configuration Steps	
AC	`Ruijie(config)#ap-config AP1` `Ruijie(config-ap)#offline-ssid my-def-ssid` `Ruijie(config-ap)#exit` `Ruijie(config)#ap-group default` `Ruijie(config-ap-group)#offline-ssid my-group-ssid`
Verification	Run the **show running** command to check whether the command is configured in all-AP and AP group configuration modes. Run the **show ap-config running** command to check the current configurations of the AP.
AC	`Ruijie(config)#show running` `!` ap-group default

	offline-ssid my-group-ssid ! Ruijie#show ap-config running ! ap-config AP1 offline-ssid my-def-ssid !

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the basic configurations of the current AC	**show ac-config**
Displays the AP backup group information	**show ac-config ap-backup-group**
Displays the BSSID list of all APs	**show ap-config bssid**
Displays the AP status information	**show ap-config cb**
Displays the WLAN information inherited by the AP	**show ap-config inherit-wlan**
Displays the AP product list	**show ap-config product**
Displays the current status of all APs	**show ap-config summary**
Displays authentication-related information of all APs	**show ap-config summary ap-auth**
Displays APs that try to associate with the AC but are rejected by the AC	**show ap-config summary deny-ap**
Displays the information about all hot backup APs associated with the AC	**show ap-config summary hot-backup**
Displays the APs in a specified AP group	**show ap-group aps**
Displays the APs in all AP groups	**show ap-group aps summary**
Displays the basic information about a specified AP	**show ap-group cb**
To display the WLAN-VLAN mapping of a specified AP group	**show ap-group intf-wlan-map**
Displays all APs	**show ap-group summary**
Displays the fit or fat mode of the AP	**show ap-mode**
Displays the basic information about a specified WLAN	**show wlan-config cb**

Description	Command
Displays the WLAN configuration list on the AC	**show wlan-config summary**

2 Configuring STA Management

2.1 Overview

STA Management (STAMG) implements station (STA) management, including STA access control management and STA event notification. Event notification is mainly used to serve other function modules. Applications of the STAMG functions are as follows:

- The dynamic blacklist is used on a security-sensitive network to prevent user attacks.
- The STA limit is used when the number of STAs exceeds the AP capacity.
- Load balancing is used when STAs need to be evenly distributed to multiple APs.
- Association control is used in the E-bag scenario.

Protocols and Standards

- N/A

2.2 Applications

Application	Description
Fit AP Networking	In fit AP network mode, at least one AC and one AP are required.
Large Conference Room	In fit AP network mode, at least one AC and two APs are required.
E-Bag	In fit AP network mode, at least one AC and two APs are required.

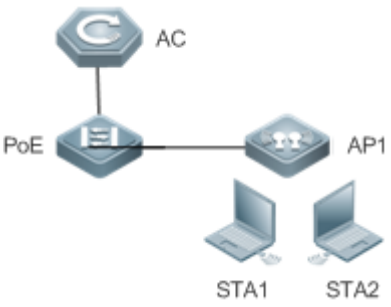
2.2.1 Fit AP Networking

Scenario

One AC is deployed on the wireless network, and dynamic blacklist and STA limit functions are enabled on the AC.

As shown in Figure 2-1, dynamic blacklist and STA limit are enabled on the AC.

Figure 2-1



Remarks	AC is the wireless access controller. PoE is the switch that functions as the gateway of APs. AP is the wireless access device. STA1 and STA2 are user devices.

Deployment

- Enable dynamic blacklist and STA limit on the AC.

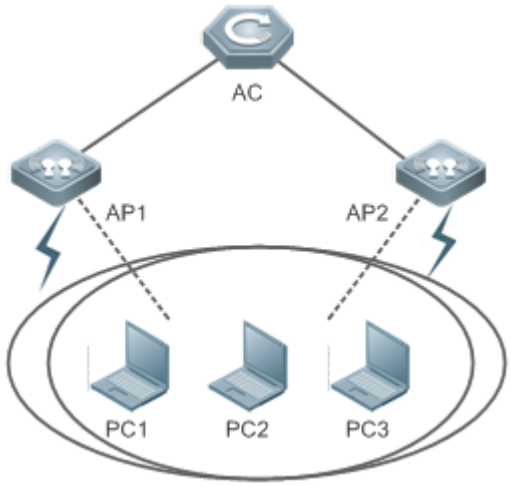
2.2.2 Large Conference Room

Scenario

In a large conference room, the number of STAs is generally large, and STAs must be evenly distributed to multiple APs; otherwise, too many STAs are connected to some specific APs, resulting in a low network speed and a poor user experience.

As shown in Figure 2-2, two APs (AP1 and AP2) are deployed in the conference room so that STAs can be evenly distributed to the two APs.

Figure 2-2



Remarks	AC is the wireless access controller. AP1 and AP2 are wireless access devices. PC1, PC2, and PC3 are user devices.

Deployment

- Enable load balancing on the AC, and add AP1 and AP2 to the load balancing group.

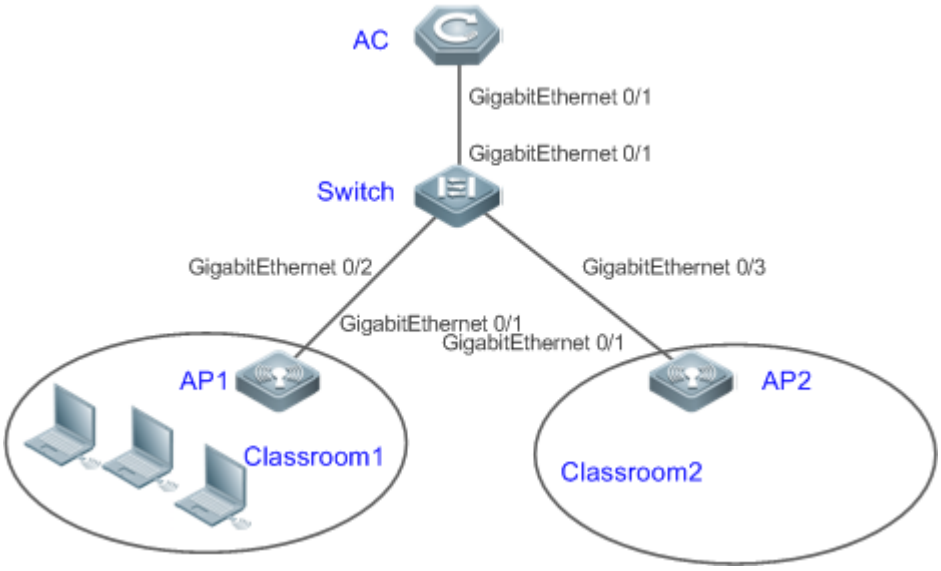
2.2.3 E-Bag

Scenario

One AC is deployed on the wireless network, and multiple APs are deployed in different classrooms. When the teacher's STA is associated with an AP, the students' STAs must also be associated with the same AP. This ensures the network transmission speed.

As shown in Figure 2-3, AP1 is deployed in Classroom1 and AP2 is deployed in Classroom2. When the teacher's STA is associated with AP1, the students' STAs must also be associated with AP1, instead of AP2. In this way, traffic destined for Classroom1 is only sent to AP1 without affecting users on AP2.

Figure 2-3



Remarks	AC is the wireless access controller. Switch functions as the gateway of APs. AP1 and AP2 are wireless access devices.

In the E-bag scenario, if the teacher uses the wired network connection, one of STAs used by students must be configured as the primary STA to implement association control. Who uses this primary STA is determined by users themselves. For example, the primary STA can be used by the class monitor or the teacher so that secondary STAs can be associated correctly. After correct association of the secondary STAs, the teacher can put this primary STA aside, and use the wired network connection during the class.

Deployment

- Enable association control on the AC, and add APs to a specified association control zone.

2.3 Features

Overview

Feature	Description
Dynamic Blacklist	Detects association of unauthorized users.
STALimit	Limits the number of STAs.
Load Balancing	Distributes STAs evenly to multiple APs.
Inter-Radio Load Balancing	Distributes STAs evenly to multiple radios of the same AP.
Association Control	Associates secondary STAs with APs in the same control zone if the primary STA is associated with these APs.
STA Management	Disassociates STAs without traffic forcibly to recycle resources.
STA Informational Syslog Suppression	Suppresses the informational syslog output rate of STAs.
Intelligent SSID Hiding	Hides the SSID when the number of STAs on an AP or radio reaches the upper limit.

2.3.1 Dynamic Blacklist

The AC can use the dynamic blacklist to punish malicious or unauthorized STAs so that these STAs cannot be associated within a period of time. In addition, the dynamic blacklist can be used to disassociate these STAs.

Working Principle

The number of STA association failures (including failures caused by incorrect user names or passwords) is counted in a period of time. When the number of association failures of an STA exceeds a certain threshold, the STA is added to the blacklist. STAs in the blacklist cannot be associated within a period of time.

2.3.2 STA Limit

STA limit aims to limit the number of STAs that can be associated with an AP based on the load capacity. This prevents the risk of insufficient resources caused by overload of APs.

Working Principle

When STAs are associated, the AP checks whether the number of associated STAs exceeds the threshold. If yes, STAs cannot be associated.

2.3.3 Load Balancing

Load balancing can balance the load among APs managed by an AC. The load here can be traffic or the number of associated STAs. The purpose is to prevent the problem that some APs are overloaded and some APs are in the idle state.

Working Principle

When an STA tries to be associated, if the load on the AP associated by the STA exceeds the preset threshold, the system checks whether the load difference between all the APs in the load balancing group of this AP exceeds the threshold. If yes, the STA is not allowed to associate with this AP. The load difference can be configured as the number of STAs or the traffic.

To prevent the problem that the STA can receive signals from only one AP but fails to be associated due to load balancing, the maximum number of load balancing times can be configured. If association fails for consecutively twice due to load balancing, load balancing is not performed for the third time and the STA can be associated with the AP.

2.3.4 Inter-Radio Load Balancing

Inter-radio load balancing can balance the load among radios of the same AP to prevent overload of a single radio. Similarly, the load here can be the traffic or the number of associated STAs.

Working Principle

The principle of inter-radio load balancing is similar to that of load balancing group except that you can configure the load balancing thresholds respectively for intra-frequency radios (2.4 GHz or 5 GHz) or inter-frequency radios. The load ratio, that is, the radio weight ratio, can be configured for radios. The default radio weight is 100. For example, if weight of radio 1 is set to 50 and that of radio 2 is set to 100, the load ratio between radio 1 and radio 2 is 1:2. When load balancing is performed, load is balanced to radio 1 and radio 2 according to this load ratio.

2.3.5 Association Control

Association control is a method for controlling association behaviors of wireless STAs. STAs are divided into two groups. In each group, only one STA is defined as the primary STA, and the other STAs are defined as secondary STAs. The secondary STAs must follow the association behaviors of the primary STA. That is, the primary and secondary STAs must be associated with the same wireless network. In this way, association behaviors of wireless STAs can be properly controlled.

Working Principle

The coverage area of a wireless network is divided into several association control zones. One or several APs are deployed in each zone, and wireless terminals are divided into groups. The control zones that can be associated with the terminals are strictly controlled. For example, a school has many classrooms, and a wireless AP is deployed in each classroom. Radio signals travel in the space. When E-bags are used in two adjacent classrooms at the same time, the ideal condition is that all the teacher and student terminals are associated with the AP of their own classrooms so that the two classrooms will not interfere with each other. In this case, a classroom must be defined as an association control zone and all the teacher and student terminals in a classroom must be associated with the AP of the classroom.

Association control aims to prevent terminals from associating with a wireless network at random when multiple wireless networks are available for selection. The following are prerequisites for network configurations:

- Based on the pre-configured association control zones and package information, the AC pushes the information about primary STAs in all packages to all APs in the association control zones and generates a whitelist of primary STAs on these APs.

- The information about primary STAs in all packages is available in the AP whitelist. Therefore, before the association control function is enabled, the primary STA must associate itself with the corresponding SSID in the specified control zone. After that, the AC pushes all corresponding secondary STAs to all APs in the association control zone and generates a whitelist according to the configuration of the primary STA package to allow the secondary STAs to associate themselves with the control zone.
- When the primary STA is de-associated from the control zone, all the secondary STAs will also be de-associated and deleted from the AP whitelist.
- The above process can be summarized as follows: The secondary STAs must follow the primary STA to associate themselves with an AP in the same control zone, with which the primary STA is associated. Only the APs of this control zone have a whitelist of the corresponding secondary STAs. This ensures that STAs are not randomly associated with APs.

2.3.6 STA Management

STA management is used to manage association and disassociation logic processing of STAs.

Working Principle

In normal cases, an STA sends a disassociation frame to inform the AC that the STA is disassociated. If the STA does not send a disassociation frame to the AC when it is disassociated abnormally (for example, because the user removes the network interface card (NIC)), the AC cannot learn the disassociation of the STA. In this case, the AC detects the STA traffic and finds that the STA has no traffic within a period of time, and concludes that the STA had been disassociated. Then, the AC performs disassociation processing on the STA.

2.3.7 STA Informational Syslog Suppression

STA informational syslog suppression prevents a high CPU usage caused by the large number of informational syslogs generated when STAs are frequently associated or disassociated.

Working Principle

The number of syslogs output per second is counted. When this number reaches the upper limit, no more syslog is output within the second, thereby suppressing the syslog. In the next second, the number of syslogs is counted again.

2.3.8 STA Jitter Prevention

The STA jitter prevention function is used to retain an STA entry on the AC for a period of time after an STA is disassociated. In this time period, if the STA goes online from the same WLAN of the AP again, it is regarded that the STA has never gone offline. If the STA goes online from the same WLAN of another AP, it is regarded that the STA roams to the AP with the same SSID. If the STA goes online from another WLAN, it is regarded that the STA is switched to another AP with a different SSID. If the AP or authentication server proactively forces an STA to go offline, the STA jitter prevention function does not take effect and the STA goes offline immediately.

The STA jitter prevention function enables an STA to perform L3 roaming, preventing a roaming failure caused by a disassociation request proactively sent by the STA in the coverage hole.

Working Principle

After the STA jitter prevention function is enabled and an STA is disassociated, the AC adds the STA to the offline queue and starts a timer according to the expected deletion time specified based on the jitter prevention time. If the STA re-associates with an AP before the timer expires, the AC removes the STA from the offline queue and regards it as an online STA. Otherwise, the AC forces the STA to go offline when the timer expires.

2.3.9 Intelligent SSID Hiding

When the number of STAs on an AP or a radio reaches the upper limit, new STAs are not allowed to go online but the STAs can still scan the SSID and attempt to perform association. After the intelligent SSID hiding function is enabled, new STAs cannot detect the signal and will not attempt to perform association.

Working Principle

When the number of STAs on an AP or a radio reaches the upper limit, the beacon frame sent by the AP does not carry the SSID. When a new STA sends a probe request, the AP does not respond with a probe response.

2.4 Configuration

Configuration	Description and Command	
Configuring Dynamic Blacklist	(Mandatory) It is used to enable the dynamic blacklist function.	
	sta-blacklist enable	Enables the dynamic blacklist function.
	(Optional) It is used to configure the parameters of the dynamic blacklist.	
	sta-blacklist lifetime	Configures the lifetime of the dynamic blacklist.
	sta-blacklist detect-time	Configures the detection time of the dynamic blacklist.
	sta-blacklist fail-limit	Configures the maximum number of association failures.
Configuring STA Limit	(Optional) It is used to configure the maximum number of STAs.	
	sta-limit	Configures the maximum number of STAs.
	sta-limit radio	Configures the maximum number of STAs that can be associated with a radio of the AP.
Configuring Load Balancing	(Mandatory) It is used to configure load balancing.	
	num-balance-group create	Creates a number-based balancing group.

	num-balance-group add	Adds an AP to the number-based balancing group.
	num-balance-group del	Deletes an AP from the number-based balancing group.
	flow-balance-group create	Creates a traffic-based balancing group.
	flow-balance-group add	Adds an AP to the traffic-based balancing group.
	flow-balance-group del	Deletes an AP from the traffic-based balancing group.
	(Optional) It is used to configure the load balancing parameters.	
	num-balance-group num	Configures the threshold of the number-based balancing group.
	num-balance-group mode	Configures the working mode of the number-based balancing group.
	flow-balance-group flow	Configures the threshold of the traffic-based balancing group.
	flow-balance-group radio-flow	Enables a specified traffic balancing group to use the traffic uploaded by APs.
Configuring Inter-Radio Load Balancing	(Mandatory) It is used to enable the load balancing function among radios.	
	inter-radio-balance flow-balance enable	Enables inter-radio traffic-based balancing.
	inter-radio-balance num-balance enable	Enables inter-radio number –based balancing.
	(Optional) It is used to configure the load balancing parameters.	
	inter-radio-balance flow-balance dual-band	Configures parameters for traffic –based balancing among inter-frequency radios.
	inter-radio-balance flow-balance same-band	Configures parameters for traffic –based balancing among intra-frequency radios.
	inter-radio-balance num-balance dual-band	Configures parameters for number-based balancing among inter-frequency radios.
	inter-radio-balance num-balance same-band	Configures parameters for number-based balancing among intra-frequency radios.

Configuring Association Control	(Mandatory) It is used to enable the association control function.	
	package	Configures a package.
	primary-sta	Configures the primary STA in the package.
	secondary-sta	Configures the secondary STA in the package.
	control-zone	Configures an association control zone.
	ap	Configures the AP information.
	assoc-control	Enables association control.
Configuring STA Management	(Optional) It is used to configure the time after which the STA is disassociated if no traffic is detected.	
	sta-idle-timeout	Configures the time after which the STA is disassociated if no traffic is detected.
Configuring STA Informational Syslog Suppression	(Optional) It is used to configure the maximum output rate of the STA informational syslogs.	
	sta-logging rate-limit	Configures the maximum output rate of the STA informational syslogs.
Configuring STA Jitter Prevention	(Optional) It is used to set the jitter prevention time.	
	prevent-jitter enable	Enables the STA jitter prevention function.
	prevent-jitter time keep-time	Configures the STA jitter prevention time.
Configuring Intelligent SSID Hiding	**hide-ssid sta-reach-limit** [**radio** { **2.4g** | **5g** }]	Configures the intelligent SSID hiding function.

2.4.1 Configuring Dynamic Blacklist

Configuration Effect

- When it is detected that the number of association failures on an STA reaches the threshold within the specified time, this STA is added to the blacklist.

Notes

- The time period is not fixed and is between **detect-time** and (**detect-time** + 5).**detect-time** is expressed in second. This factor must be considered during configuration.

- If multiple authentication modes are applied, the number of STA association failures increases by 1 so far as one of the authentication modes fails. Combinations of authentication modes include, but are not limited to, PSK+Web, PSK+MAB+Web, PSK+MAB, MAB+Web, and 802.1x+Web.

Configuration Steps

Enabling Dynamic Blacklist

- (Mandatory) Enable the dynamic blacklist function on an AC or a fat AP.

Command	**sta-blacklist enable**
Parameter Description	N/A
Defaults	The blacklist function is disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring the Dynamic Blacklist Parameters

- (Optional) Configure the dynamic blacklist parameters on an AC or a fat AP.
- Configure the blacklist lifetime.
- Run the **sta-blacklist lifetime** command to configure the lifetime of the dynamic blacklist. A longer lifetime indicates a longer period of time within which the STA added to the blacklist is not allowed to associate itself with the AC.
- Run the **sta-blacklist detect-time** command to configure the detection time. As the detection time decreases, the unauthorized STA detection becomes more sensitive and the number of false reports increases.
- Run the **sta-blacklist fail-limit** command to configure the upper limit of association failures. A larger upper limit indicates that an STA can make more association attempts.

Command	**sta-blacklist lifetime** *seconds*
Parameter Description	*seconds:* Indicates the blacklist lifetime. The value ranges from 60s to 1200s.
Defaults	300s
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**sta-blacklist detect-time** *seconds*
Parameter Description	*seconds:* Indicates the STA detection time. The value ranges from 5s to 60s.
Defaults	60s
Command Mode	AC configuration mode

Usage Guide	This command is used to configure the STA detection time. When encountering the first association failure, the STA is listed as a suspected attacker. If the number of association failures on the STA reaches the upper limit (namely, the **fail-limit**) within the detection time, the STA is added to the blacklist.

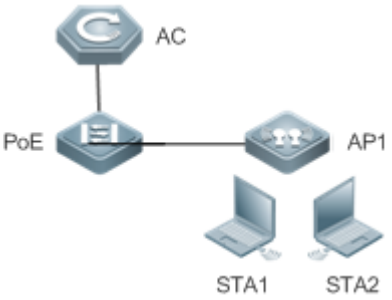
Command	**sta-blacklist fail-limit** *number*
Parameter Description	*number*: Indicates the maximum number of association failures. The value ranges from 1 to 100.
Defaults	5
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show sta-blacklist** command to display the STAs in the blacklist.

Configuration Example

Configuring Dynamic Blacklist

Scenario **Figure 2-4**	
Configuration Steps	● Configure the dynamic blacklist function.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-blacklist enable
Verification	● After the CAPWAP tunnel is established between an AP and an AC, enter an incorrect password for several times to verify that the STA can be added to the blacklist.
AC	AC# show sta-blacklist

	Num STA MAC Add time ---------- -------------- -------------------- 1 0080.1111.1111 2013-07-02 13:56:22 2 0090.2222.3333 2013-07-02 13:56:35 3 0070.1111.2233 2013-07-02 13:57:08

Common Errors

- N/A

2.4.2 Configuring STA Limit

Configuration Effect

- Limit the maximum number of STAs that can be associated with an AC, a WLAN, an AP, or a radio of an AP on the wireless network.

Notes

- The STA limits configured for an AC, a WLAN, an AP, or a radio of an AP take effect simultaneously. That is, an STA can be associated only if all the STA limits are met.
- The STA limit configured on the AC is subject to the license.

Configuration Steps

↘ Configuring STA Limit

- (Optional) Configure the STA limitation an AC or a fat AP.
- If the number of STAs on the wireless network is large, the STA limit can be configured to allow more STAs are associated, but the total bandwidth will decrease.
- Run the **sta-limit** command to configure the STA limit. A large STA limit indicates that more STAs can be associated.
- The AC-based STA limit is (32 x Number of APs) by default. The WLAN-based STA limit is not specified by default. The AP-based STA limit is 32 by default.
- Run the **sta-limit radio** command to configure the radio-based STA limit for an AP. A large STA limit indicates that more STAs can be associated.
- Run the **sta-limit per-ap** command to configure the maximum number of STAs supported on each AP in a WLAN. By default, the number of STAs on an AP is not limited. If the number of configured STAs exceeds the maximum number of STAs supported by an AP, no new STA can associate with the AP.

Command	**sta-limit** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of STAs. The value varies according to the configuration mode and device.

Defaults	In AC configuration mode, the default value is (32 x Number of APs supported by the AC), depending on the license. In AP group configuration mode, the default value is 32. In AP configuration mode, the default value is 32 for a disassociated AP or in the **ap-config all** configuration mode. The default value for an associated AP is determined by the AP model. In WLAN configuration mode, the STA limit is not specified.
Command Mode	AC configuration mode, WLAN configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

Command	**sta-limit** *max-num* **radio** *radio-id*
Parameter Description	*max-num*: Indicates the maximum number of STAs. The value ranges from 1 to 156. *radio-id*: Indicates the radio ID. The value ranges from 1 to 32.
Defaults	The STA limit is not specified by default.
Command Mode	AP configuration mode AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity of the radio, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

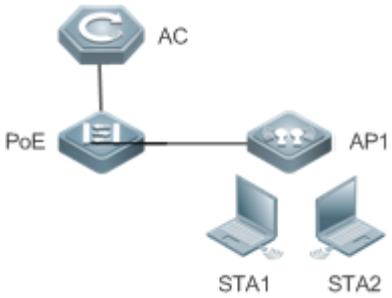
Command	**sta-limit per-ap** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of STAs supported on an AP. The value ranges from 1 to 1536.
Defaults	By default, the number of STAs supported on an AP is not limited.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Verify that the number of STAs is limited.

Configuration Example

Configuring STA Limit

Scenario **Figure 2-5**	
Configuration Steps	● Configure the STA limit.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-limit64
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the AC running configuration.
AC	AC# show ap-config running ap-config ap1 sta-limit 64 !

Common Errors

- N/A

2.4.3 Configuring Load Balancing

Configuration Effect

- Enable even distribution of STAs on multiple APs in a load balancing group.

Notes

- Load balancing is applicable only to STAs that are associated, but not to STAs that are disassociated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.
- Load balancing takes effect only on the same type of radios (2.4 GHz or 5 GHz). If the types of radios are different, load balancing is performed only when the AP reports that the STAs are capable of dual-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio.

- After the traffic-based balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs and is not routed to the AC. During this interval, the traffic information on the AC does not change. At this time, if the traffic between APs is not balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.

Configuration Steps

Creating a Number-based Balancing Group

- (Mandatory)Create a number-based balancing group on the AC.
- APs can be only added to a created load balancing group.

Command	**num-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No number-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Number-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing applies to the APs which are added to the load balancing group.

Command	**num-balance-group add** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the number-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Creating a Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- APs can be only added to a created load balancing group.

Command	**flow-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No traffic-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing applies to the APs which are added to the load balancing group.

Command	**flow-balance-group add** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the traffic-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring Parameters of Load Balancing Group

- (Optional) Configure the parameters of load balancing group on the AC.
- Run the **num-balance-group num** command to configure the threshold of number-based balancing group. A larger threshold indicates a greater difference in the number of STAs associated with two APs, and the less balanced load.
- Run the **num-balance-group mode** command to configure the radio-based balancing function. If radio-based balancing is enabled, the control on the distribution of STAs is more accurate, but the effect of balancing among APs is less satisfying.
- Run the **num-balance-group enable** command to configure the trigger threshold of the number-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavy.
- Run the **num-balance-group del** command to delete an AP from the number-based balancing group.
- Run the **flow-balance-group flow** command to configure the traffic-based balancing threshold. A higher traffic balancing threshold indicates that the traffic difference between two APs is greater and the traffic is less balanced.
- Run the **flow-balance-group radio-flow** command to enable the traffic balancing group to use the traffic information uploaded by APs. In local forwarding mode, data packets are not routed to the AC, and the AC cannot obtain the traffic information. Therefore, the traffic information uploaded by APs must be used to determine whether to enable load balancing.
- Run the **flow-balance-group enable** command to configure the trigger threshold of the traffic-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavy.
- Run the **flow-balance-group del** command to delete an AP from the traffic-based balancing group.
- Run the **flow-balance-group base** command to configure the baseline of traffic balancing in global configuration mode.
- Run the **sta-balance num-limit enable** command to limit the maximum times of load balancing.

Command	**num-balance-group num** *group-name number*
Parameter Description	group-name: Indicates the name of a load balancing group. number: Indicates the trigger threshold. The default value is 3. The value ranges from 0 to 20, where 0 indicates that the number balancing function is disabled for the load balancing group.
Defaults	3

Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group mode** *group-name*{ **radio-mode**| **ap-mode** }
Parameter Description	*group-name:* Indicates the name of a load balancing group.
Default s	AP-based number balancing
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The default value is 3. The value ranges from 0 to 10, where 0 indicates that the number balancing function is disabled for the load balancing group.
Defaults	3
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group del** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group flow** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 1000, where 0 indicates that the load balancing function is disabled for the load balancing group. The percentage baseline is 10 Mbps by default.
Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group radio-flow** *group-name*
Parameter Description	*group-name:* Indicates the name of the traffic balancing group.
Defaults	Traffic information on the CAPWAP data channel is used on the AC.
Command Mode	AC configuration mode
Usage Guide	You can enable a traffic balancing group to use the traffic information uploaded by APs. In this way, the traffic balancing group can receive the traffic information periodically sent by APs for load balancing.

Command	**flow-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: Indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 500, where 0 indicates that the load balancing function is disabled for the load balancing group. The percentage baseline is 10 Mbps by default.
Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group del** *group-name ap-name*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *ap-name:* Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group base** *number*
Parameter Description	*number*: Indicates that traffic baseline. The default value is 10 Mbps. The value ranges from 1 to 100.
Defaults	10 Mbps
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**sta-balance num-limit enable**

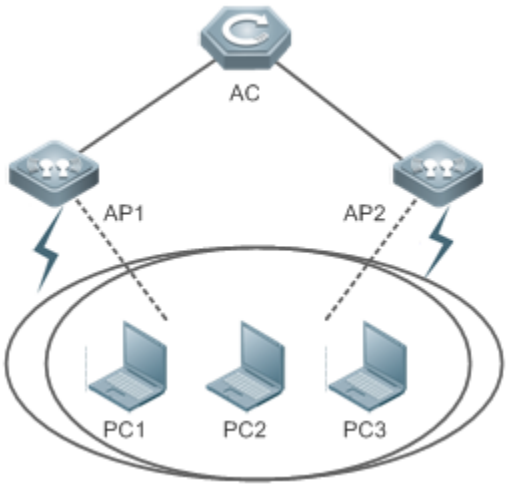
Parameter Description	N/A
Defaults	The function is disabled by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Number balancing: Check whether the difference in the number of STAs associated with APs in the load balancing group is within the threshold.
- Traffic balancing: Check whether the difference in the traffic of APs in the load balancing group is within the threshold.

Configuration Example

Configuring Traffic Balancing

Scenario **Figure 2-6**	
Configuration Steps	● Create a load balancing group. ● Set the trigger threshold of this load balancing group to 1000 Kbps. ● Add AP1 and AP2 to the load balancing group named **test-group.** (If two APs are added to the same load balancing group, PCs in this group can search the RF signals of all APs.)
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ac-controller AC(config-ac)#flow-balance-group create test-group AC(config-ac)#flow-balance-group flow test-group 10 AC(config-ac)#flow-balance-group add test-group AP1

	AC(config-ac)#flow-balance-group add test-group AP2
Verification	● Check the configuration of the load balancing group.
AC	AC# show ac-config flow-balance summary Group State Enable Threshold Base mode AP NAME --- --- --- --- --- --- test-group UP 5*100kbps 10% 10 ap-mode(0) AP1, AP2

Common Errors

- N/A

2.4.4 Configuring Inter-Radio Load Balancing

Configuration Effect

- Enable inter-radio load balancing on APs to balance the load among radios.
- Configure the load ratio of radios. Load between radios is balanced according to the ratio.

Notes

- This function is not applicable to the i-Share solution. Signals of different radios cover different areas. An STA may receive signals from one or several radios. In this case, the inter-radio load balancing function cannot be enabled.
- Load balancing is applicable only to STAs that are associated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.
- If the radio that an STA attempts to associate with is different from the radio with the lowest load, load balancing is performed only when the AP reports that the STA is capable of dual-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio.
- After the traffic balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs in local forwarding mode. During this interval, the traffic information on the AC does not change. At this time, if the traffic between APs is not balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.
- Configuration of load balancing parameters varies according to the inter-frequency and intra-frequency radios.
- When performing load balancing, determine the load balancing parameter according to the target radio and the type of the radio associated with the STA. Then, determine whether to associate the STA to the target radio. For a specific AP, so far as load balancing is enabled in any of the ap-config, ap-group, and ap-config all modes, load balancing is enabled on this AP. If the load balancing configurations in the three modes are different, the configurations take effect in the following sequence: ap-config > ap-group > ap-config all.

- When inter-radio load balancing is enabled, the association attempt of the same STA will be denied for at most twice within five minutes. If the STA is still associated with a radio with a heavy load for the third time, the association is allowed. Therefore, the effect of inter-radio load balancing is related to the actual STA behaviors.

Configuration Steps

Enabling Inter-radio Traffic Balancing

- (Mandatory). The configuration is performed on the AC. After the function is enabled, traffic is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured in ap-config all mode).

Command	**inter-radio-balance flow-balance enable**
Parameter Description	N/A
Defaults	Inter-radio traffic balancing is disabled.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Enabling Inter-radio Number Balancing

- (Mandatory)The configuration is performed on the AC. After the function is enabled, the number of STAs is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured in ap-config all mode).

Command	**inter-radio-balance num-balance enable**
Parameter Description	-
Defaults	Inter-radio number balancing is disabled.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Configuring Inter-radio Load Balancing Parameters

- (Optional) The configuration is performed on the AC. Parameters can be adjusted based on actual requirements of network optimization.
- Run the **inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.

- Run the **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.

Command	**inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The unit is 100 kbps. The value ranges from 1 to 1000. thrs-num: Indicates the load threshold. The unit is 100 Kbps. The value ranges from 1 to 1000.
Defaults	By default, both the trigger threshold and the load threshold are 10.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance flow-balance same-band enable-load***e n-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The unit is 100 kbps. The value ranges from 1 to 1000. thrs-num: Indicates the load threshold. The unit is 100 Kbps. The value ranges from 1 to 1000.
Defaults	By default, both the trigger threshold and the load threshold are 5.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The value ranges from 1 to100. thrs-num: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	By default, both the trigger threshold and the load threshold are 8.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	en-num: Indicates the trigger threshold. The value ranges from 1 to 100. thrs-num: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	By default, both the trigger threshold and the load threshold are 20 and 6 respectively.
Command Mode	AP configuration mode, AP group configuration mode

Usage Guide	N/A

Configuring the Load Ratio of Radios

- (Optional) The configuration is performed on the AC. After the load ratio is configured, load is balanced to different radios of the same AP based on the ratio.
- The load ratio can be configured for a single AP, all APs in an AP group, or all APs (ap-configure all configuration mode).

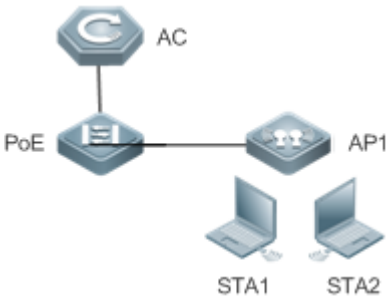
Command	**inter-radio-balance radio** *radio-id* **weight** *weight-num*
Parameter Description	N/A
Defaults	The radio weight is 100, and load is balanced between radios based on the 1:1 ratio by default.
Command Mode	AP configuration mode, AP group configuration mode
Usage Guide	N/A

Verification

- Number balancing: Run the **show ap-config summary** command to check whether the difference in the number of STAs between radios of the AP where load balancing is within the threshold.
- Traffic balancing: Run the **show ac-config client** command to check whether the traffic difference between radios of the AP where load balancing is enabled is within the threshold.

Configuration Example

Enabling Inter-radio Number Balancing on All APs in the Default AP Group

Scenario Figure 2-7	
Configuration Steps	● Enter the default AP group configuration mode. ● Enable inter-radio number balancing.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ap-group default AC(config-group)#inter-radio-balance num-balance enable

Verification	• Run the **show run** command and check the configurations.
AC	AC# show run | begin ap-group default ap-group default inter-radio-balance num-balance enable

Common Errors

- N/A

2.4.5 Configuring Association Control

Configuration Effect

- Secondary STAs must be associated with APs in the same group as the primary STA when being associated.

Notes

- When a package is deleted, all its related configurations are deleted as well. If some STAs in this package are currently associated, all these STAs will be disassociated.
- A package can only be configured with one primary STA. If the information about the primary STA in the package is configured for multiple times, the latest configuration prevails.
- When a primary STA is deleted from a package, the primary STA and all secondary STAs in this package may be disassociated.
- When a secondary STA is deleted from a package, this secondary STA may be disassociated.
- The association control zone name cannot be duplicated; otherwise, an error will be prompted. In addition, if an association control zone is deleted, all configurations related to this zone will be deleted. Consequently, STAs in the package associated with this control zone may be disassociated.
- When the AP information in an association control zone is deleted, STAs in the package associated with this AP be disassociated.

Configuration Steps

↘ Configuring a Package

- (Mandatory) The configuration is performed on an AC or a fat AP.
- The primary and secondary STA information can be configured only after a package is configured.

Command	**package** *pkg-name*
Parameter Description	*pkg-name*: Indicates the name of a package. The package name is a string of 1 to 32 characters.
Defaults	No package is configured by default.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuring the Primary and Secondary STAs in a Package

- (Mandatory) The configuration is performed on an AC or a fat AP.
- Run the **primary-sta** command to configure the primary STA. Only one primary STA can be configured. The secondary STAs will be associated with APs in the same group as the primary STA.
- Run the **secondary-sta** command to configure a secondary STA. After the secondary STA is configured, the secondary STA will be associated with an AP in the same group as the primary STA.

Command	**primary-sta** *mac-address*
Parameter Description	*mac-address*: Indicates the MAC address of the STA.
Defaults	No primary STA is configured by default.
Command Mode	Package configuration mode
Usage Guide	N/A

Command	**secondary-sta** *mac-address*
Parameter Description	*mac-address*: indicates the MAC address of the STA.
Defaults	No secondary STA is configured by default.
Command Mode	Package configuration mode
Usage Guide	-

Configuring an Association Control Zone

- (Mandatory) The configuration is performed on an AC or a fat AP.
- Configure an association control zone.
- APs can be added to an association control zone only after this association control zone is configured.

Command	**control-zone** *czone-name*
Parameter Description	*czone-name*: Indicates the name of an association control zone. The name is a string of 1 to 64 characters.
Defaults	No association control zone is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding an AP to an Association Control Zone

- (Mandatory) The configuration is performed on an AC or a fat AP.

- Add an AP to an association control zone.
- Association control can be performed on only APs that are added to the association control zone.

Command	**ap** *WORD*
Parameter Description	*WORD*: Indicates the name of an AP. The name is a string of 1 to 64 characters.
Defaults	No AP is added to an association control zone by default.
Command Mode	Association control zone configuration mode
Usage Guide	N/A

Enabling the Association Control Function

- (Mandatory) The configuration is performed on an AC or a fat AP.The **assoc-control** command must be used to enable the association control function.
- Enable the association control function.

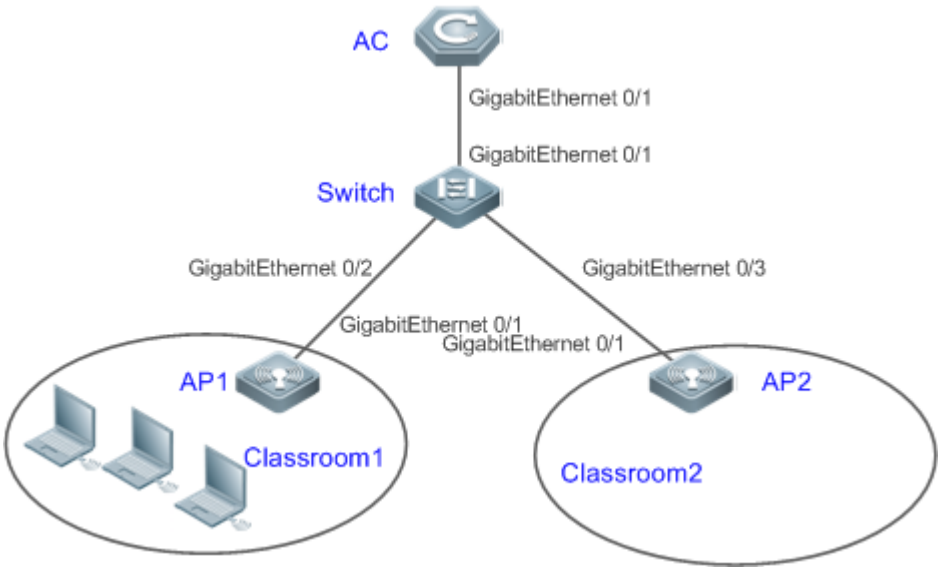
Command	**assoc-control**
Parameter Description	N/A
Defaults	The association control function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Verify that secondary STAs can be associated with APs in the same group as the primary STA.

Configuration Example

Configuring the E-bag in Fit AP Structure.

Scenario **Figure 2-8**	
Configuration Steps	● Configure packages and related primary STAs and secondary STAs. ● Configure association control zones and related APs. ● Enable the association control function.
AC	AC#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# package Cart 1 AC(config-package)#primary-sta 00d0.f800.0001 AC(config-package)#secondary-sta 00d0.f800.0002 AC(config-package)#secondary-sta 00d0.f800.0003 AC(config-package)#exit AC(config)# control-zone Classroom 1 AC(config-czone)#apAP1 AC(config-czone)#exit AC(config)# control-zone Classroom 2 AC(config-czone)# apAP2 AC(config-czone)#exit AC(config)#assoc-control
Verification	● Display the association control running state. ● Display the package configuration. ● Display the association control zone configurations.

AC	AC#show assoc-control Association control is enabled. AC# show package total package num : 1 ========= Cart 1 ========= primary STA : 00d0.f800.0001 secondary STA num : 2 00d0.f800.0002 00d0.f800.0003 AC# show control-zone control zone num : 2 control-zoneAP ------------ ---------- Classroom 1 AP1 00d0.f800.889e Classroom 2 AP2 00d0.f800.889f

Common Errors

- N/A

2.4.6 Configuring STA Management

Configuration Effect

- STAs are disassociated if no traffic is detected on the STAs within the specified time.

Notes

- N/A

Configuration Steps

Configuring the STA Aging Time

- (Optional) The configuration is performed on an AC or a fat AP.
- A shorter time configured indicates that an STA without traffic can be detected and disassociated in a faster manner.

Command	**sta-idle-timeout** *value*
Parameter Description	*value*: Indicates the aging time in second. The value ranges from 60 to 86400.
Defaults	300s

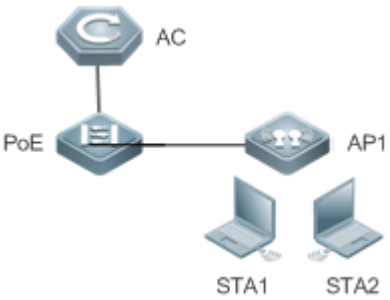
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Check whether the STA aging time is successfully configured.

Configuration Example

Configuring the STA Aging Time

Scenario **Figure 2-9**	
Configuration Steps	● Configure the STA aging time.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-idle-timeout 15
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	AC# show ap-config running ap-config ap1 sta-idle-timeout 15 !

Common Errors

- N/A

2.4.7 Configuring STA Informational Syslog Suppression

Configuration Effect

- Even STAs are frequently associated or disassociated, the number of informational syslogs output per second does not exceed the limit.

Notes

- N/A

Configuration Steps

Configuring the Syslog Suppression Rate

- (Optional) The configuration is performed on the AC.
- Configure the syslog suppression rate. A larger rate configured indicates that more syslogs can be output per second.

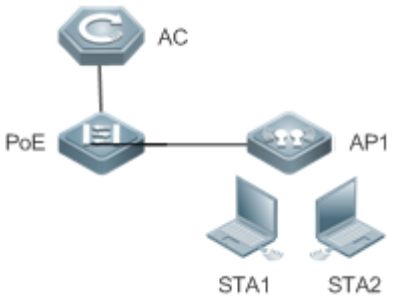
Command	**sta-logging rate-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the rate, which is expressed in records per seconds. The value ranges from 0 to 10000.
Defaults	By default, less than five syslog records are output per second, that is, the maximum syslog output rate is 5 records per second.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Configuring the STA Informational Syslog Suppression Function

Scenario **Figure 2-10**	
Configuration Steps	● Configure the STA informational syslog suppression function.

AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-logging rate-limit 50
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	AC# show running ac-controller sta-logging rate-limit 50 !

Common Errors

- N/A

2.4.8 Configuring STA Jitter Prevention

Configuration Effect

- After the STA jitter prevention function is enabled for a WLAN and an STA is disassociated from the WLAN, the AC retains an STA entry for a period of time before forcing the STA to go offline.

Notes

- When an AC or authentication server proactively forces an STA to go offline, the STA jitter prevention function does not take effect.

Configuration Steps

↘ Enabling the STA Jitter Prevention Function

- (Mandatory) Enable the STA jitter prevention function on the AC.

Command	**prevent-jitter enable**
Parameter Description	N/A
Defaults	The STA jitter prevention function is disabled by default.
Command Mode	WLAN configuration mode

Usage Guide	After the STA jitter prevention function is enabled for a WLAN and an STA is disassociated from the WLAN, the AC retains an STA entry for a period of time (60s by default) before forcing the STA to go offline.

Configuring the STA Jitter Prevention Time

- (Optional) Configure the STA jitter prevention time on the AC.

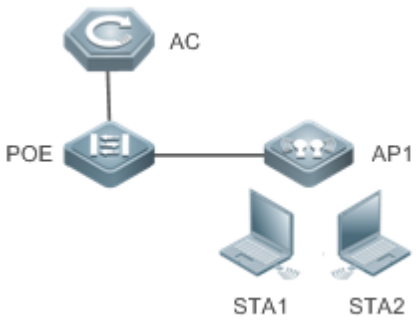
Command	**prevent-jitter time** *keep-time*
Parameter Description	*keep-time*: indicates the STA jitter prevention time in seconds. The value ranges from **1** to **86400**.
Defaults	60
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Enabling the STA Jitter Prevention Function

Scenario **Figure 2-11**	
Configuration Steps	Enable the STA jitter prevention function.
AC	`AC# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `AC(config)# wlan-config 1`

	AC(config-wlan)# prevent-jitter enable
Verification	Check the configuration information.
AC	AC# show running-config wlan-config 1 SSID prevent-jitter enable !

Common Errors

- N/A

2.4.9 Configuring Intelligent SSID Hiding

Configuration Effect

- When the number of STAs on an AP or a radio reaches the upper limit, new STAs cannot detect the SSID.

Notes

- This function takes effect only when both the AC and AP versions support this function.

Configuration Steps

↘ Enabling Intelligent SSID Hiding

- (Optional) The configuration is performed on the AC.
- Enable the intelligent SSID hiding function.

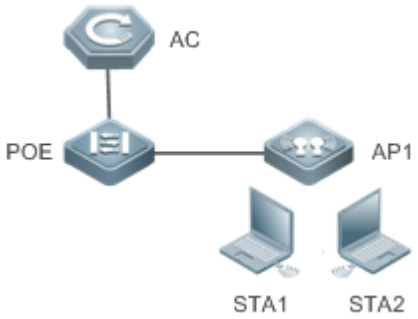
Command	**hide-ssid sta-reach-limit [radio { 2.4g | 5g }]**
Parameter Description	**radio**: indicates a specific radio on which the intelligent SSID hiding function is enabled. If this parameter is not specified, the intelligent SSID hiding function is enabled on all radios. **2.4g**: indicates that the intelligent SSID hiding function is enabled on the 2.4G radio. **5g**: indicates that the intelligent SSID hiding function is enabled on the 5G radio.
Defaults	The intelligent SSID function is disabled by default.
Command Mode	AP configuration mode
Usage Guide	After the intelligent SSID function is enabled and the numbers of STAs on all APs in an area reach the upper limit, new STAs cannot detect the SSID in this area.

Verification

- Run the **show running** or **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Enabling Intelligent SSID Hiding Function

Scenario **Figure 2-12**	
Configuration Steps	Enable the intelligent SSID hiding function.
AC	`AC# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `AC(config)# ap-config AP1` `AC(config-ap)# hide-ssid sta-reach-limit`
Verification	After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	`AC# show ap-config running AP1` `ac-config AP1` ` hide-ssid sta-reach-limit` `!`

Common Errors

- The AC version supports the intelligent SSID hiding function but the AP version does not.

2.5 Monitoring

Displaying

Description	Command
Displays the information about all STAs connected to the AC.	**show ac-config client** [**by-ap-name | 802.11a | 802.11b | 802.11n | 802.11g** | **802.11ac | 802.11ax | other**]
Displays the detailed information about a specified STA.	**show ac-config client detail** *mac-address*
Displays the statistics of all STAs.	**show ac-config client statistic**
Displays the detailed configuration of the traffic-based balancing group.	**show ac-config flow-balance summary**
Displays the detailed configuration of the number-based balancing group.	**show ac-config num-balance summary**
Displays the status of the association control function.	**show assoc-control**
Displays the association control zone configuration.	**show control-zone** [**summary** | *czone-name*]
Displays the package configuration.	**show package** [*pkt-name*]
Displays the STAs in the blacklist.	**show sta-blacklist**
Displays the 802.11ac wave2 information.	**show ac-config client 11ac-wave2**
Displays the backup information of an STA.	**show ac-config client hot-backup**

3 Configuring CAPWAP

3.1 Overview

Control And Provisioning of Wireless Access Points (CAPWAP) is a protocol proposed to address the issue of large-scale access point (AP) deployment on the wireless local area network (WLAN).

On a fit AP network, the access controller (AC) manages all APs in a unified manner through CAPWAP. The AC pushes control polices to specified APs, instead of configuring APs one by one. CAPWAP is used to set up the control channel and the data channel between an AP and an AC. The control channel is used by ACs to configure APs, or by APs to send event notifications to ACs. The data channel is used to exchange data packets between APs and ACs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

3.2 Applications

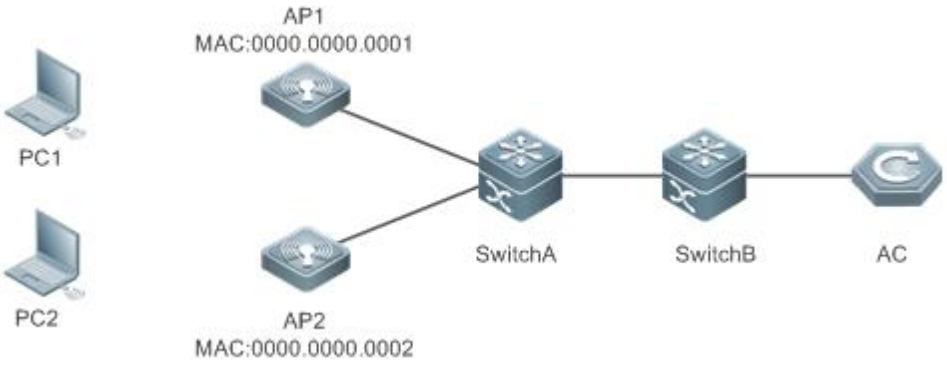
Application	Description
Dynamically Setting up a CAPWAP Tunnel	An AP accesses an AC through switches. The DCHP server is deployed on the switch connected to APs. The AP obtains the AC address dynamically through DHCP to set up a CAPWAP tunnel with the AC.
Statically Setting up a CAPWAP Tunnel	An AP accesses an AC through switches. The static IP address of the AC is configured on the AP. The AP sets up a CAPWAP tunnel with the AC based on the configured static IP address of the AC.
Upgrading APs	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale through CAPWAP.

3.2.1 Dynamically Setting up a CAPWAP Tunnel

Scenario

APs access the AC through switches. The DCHP server is deployed on the switch connected to APs. On the DHCP server, the DHCP address pool is configured and Option138 is pushed, where Option138 is the IP address of the AC. The AP obtains the AC address and sets up a CAPWAP tunnel with the AC. As shown in Figure 3-1, the AC, switches (SwitchA and SwitchB), and APs (AP1 and AP2) are connected with each other through the trunk ports. PC1 is connected to AP1, and PC2 is connected to AP2.

Figure 3-1



Deployment

- APs do not need to be configured one by one on a fit AP network. When an AP is powered on, the IP address must be obtained first. Therefore, a DHCP server must be deployed on the network. If the DHCP server is not deployed, the DHCP function of the AC is used to implement functions of the DHCP server.
- The AC communicates with the AP through the Layer3 (L3) switch, and the DHCP server must send Option138, which contains the IP address of the AC. After obtaining the IP address of the AC, the AP sets up a CAPWAP communication tunnel with the AC.
- On the AC, configure a loopback interface address, or run the **capwap ctrl-ip** *ip-address* command to configure the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.

3.2.2 Statically Setting up a CAPWAP Tunnel

Scenario

The AP sets up a CAPWAP tunnels with the AC based on the configured static IP address of the AC. An AP accesses an AC through switches. The topology is the same as that shown in Figure 3-1.

Deployment

- Configure the static IP addresses of ACs. The AP will send the Discover Request messages to these static IP addresses to check the effectiveness of ACs, and then select and join an AC.
- On the AC, configure a loopback interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.

3.2.3 Upgrading APs

Scenario

The AP obtains the AC address based on the configured static IP address of the AC or from the DHCP server, and sets up a CAPWAP tunnel with the AC. The AP accesses the AC through switches. The topology is the same as that shown in Figure 3-1.

Deployment

- On the AC, configure an IP interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interworking between the AC and the IP address obtained by the AP.
- On the AC, activate the AP software that is stored locally.

3.3 Features

Basic Concepts

STA, AP, and AC

STA: It is a wireless workstation that is equipped with the wireless network interface card (NIC), such as a laptop computer or a mobile phone.

AP: It is a wireless access point that provides radio signals so that the STA can access the wireless network.

AC: It is a wireless access controller that provides wireless connection and related service functions.

Control Channel and Data Channel

Control channel: It is used by ACs to configure APs, or by APs to send event notifications to ACs.

Data channel: It is used to exchange data packets between APs and ACs.

AC Discovery

AC discovery phase: An AP can send a discover request message by means of broadcast, multicast, DHCP, DNS, or static configuration to detect ACs, select an optimum AC from one or more ACs, join the AC, and set up a CAPWAP session with the AC.

Datagram Transport Layer Security (DTLS)

The CAPWAP control channel uses the DTLS protocol for key negotiation and encryption.

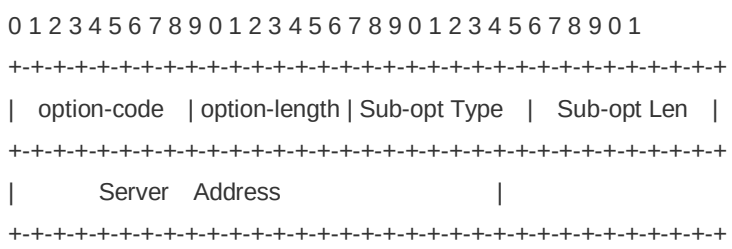
Option

The Option information sent by the DHCP server can carry the IPv4 or IPv6 address of an AC. The AP obtains the AC address from the Option information sent by the DHCP server.

The AP can obtain the IP address of an AC using Option 138 or Option 43, or obtain the IPv6 address of an AC using Option 52. When configuring the DHCP server of the AP, you must configure the related options to set the IP address of the AC; otherwise, the AP cannot discover the AC through DHCP discovery.

Option 138 and Option 52 are standard formats defined in RFC5417, and Option 43 is defined by vendors. Currently, Option 43 in the following formats can be analyzed:

Format 1: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is Option 43 hex f10401010101.



option-code: indicates the option code. In this example, the option code is 43 in decimal format.

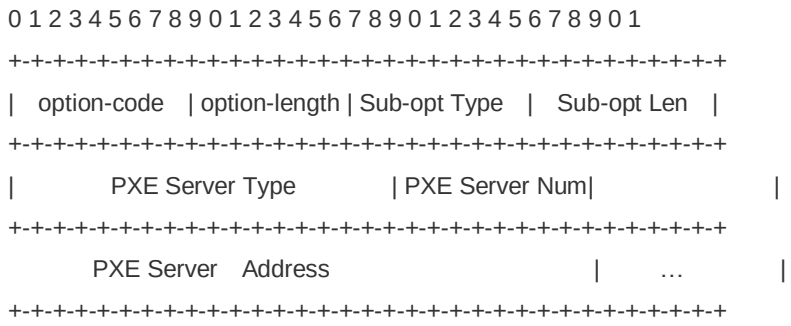
option-length: indicates the length of the option data, which excludes option-code and option-length.

Sub-opt Type: indicates the sub-option type. In this example, the sub-option type is 0xF1, that is, 241 in decimal format.

Sub-opt Len: indicates the length of the sub-option, which is equal to (Number of addresses x 4).

Server Address: indicates the server address.

Format 2: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 800700000101010101.



option-code: indicates the option code. In this example, the option code is 43 in decimal format.

option-length: indicates the length of the option data, which excludes option-code and option-length.

Sub-opt Type: indicates the sub-option type. In this example, the sub-option type is 0x80, that is, 128 in decimal format.

Sub-opt Len: indicates the length of the sub-option, which is equal to (Number of addresses x 4 +3).

Server Type: indicates the server type. The value is 0x0000.

Server Num: indicates the number of server addresses.

Server Address: indicates the server address.

Format 3: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 01010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length | Server   Address            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Server   Address           |               …   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: indicates the option code. In this example, the option code is 43 in decimal format.

option-length: indicates the length of the option data, which excludes option-code and option-length.

Server Address: indicates the server address.

Overview

Feature	Description
Discovering an AC by an AP	The AP discovers potential ACs.
Joining an AC by an AP	The AP selects an optimum AC from one or more ACs, joins the AC, and sets up a CAPWAP tunnel with the AC.
Upgrading APs	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale.
Forwarding Data on the Tunnel	After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged through the data channel.

3.3.1 Discovering an AC by an AP

An AP discovers potential ACs by sending a Discovery Request message.

Working Principle

As soon as an AP is connected to the network, the AP enters the process of discovering ACs. The AP sends a Discovery Request message by means of broadcast, multicast, or unicast If unicast is used, the AP obtains the AC IP address list through the DHCP server, DNS, or configuration of the static AC IP addresses.

3.3.2 Joining an AC by an AP

The AP selects an optimum AC from one or more ACs, joins the AC, and sets up a CAPWAP tunnel with the AC.

Working Principle

The AP sends a Discovery Request message to ACs. ACs that receive the Discovery Request message return a Discovery Response message to the AP. Among the ACs that send the response message, the AP selects an optimum AC, and sets up a DTLS connection with this AC. After the DTLS connection is successfully set up, the AP sends a Join Request message. The

AC returns a Join Response message to confirm that the AP is added to the management scope of the AC, and starts to provide services for this AP.

3.3.3 Upgrading APs

After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in a large scale.

Working Principle

After an AP joins an AC, if the AP firmware version expires, the AP enters the firmware upgrade process. The AP downloads the latest firmware version from the AC, restarts after the successful upgrade, and reinitiates an AC discovery process. If the AP firmware is of the latest version, the AP downloads configuration parameters from the AC and starts running. Figure 3-2 shows the working principle.

Figure 3-2

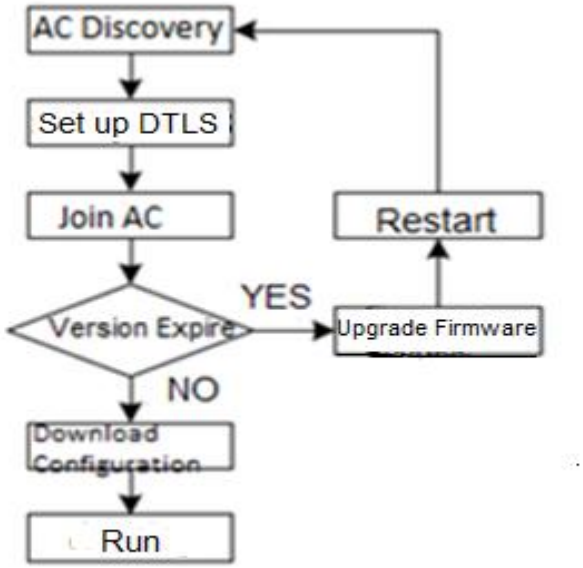
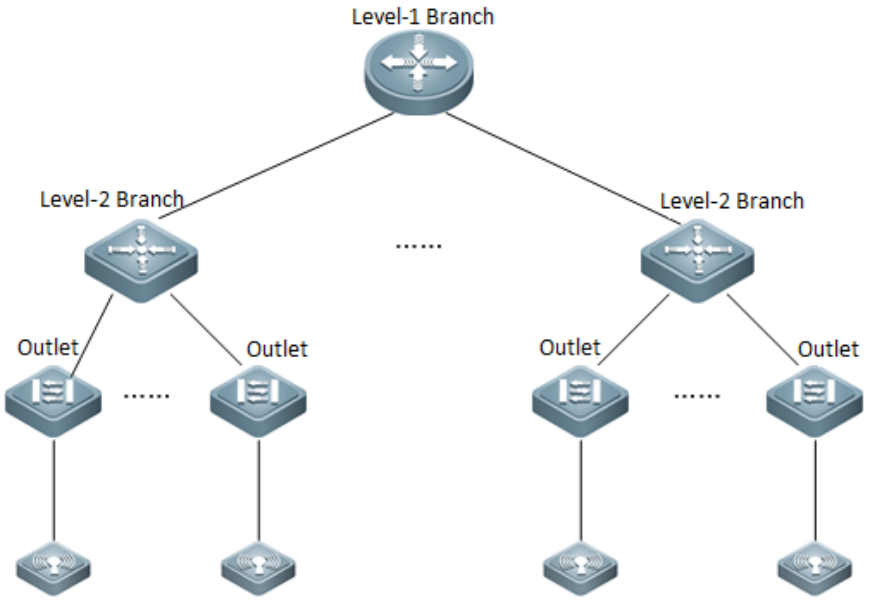


Figure 3-3 shows the typical upgrade scenario where the bandwidth is limited.

Figure 3-3



The following explains the configuration method for upgrading APs in a bank. Assume that the bank consists of one level-1 branch and multiple level-2 branches, and each branch has hundreds of outlets. One AP is deployed in one outlet, and the AC is deployed in the level-1 branch. The bandwidth between the level-1 bank and the level-2 bank is 20 Mbps, and the bandwidth between the level-2 bank and the outlet is 2 Mbps. To prevent affecting normal service provisioning of the bank, the bandwidth occupied by the AP upgrade process cannot exceed 50% of the total available bandwidth. Assume that there are eight level-2 branches, eight upgrade groups are configured on the AC, and APs of outlets under each level-2 branches are added to the corresponding upgrade group. For each AP, the maximum available bandwidth is 1 Mbps. Therefore, a bandwidth of 128 Kbps (1MByte = 128KByte) should be configured for each AP. Under each level-2 branch, the number of APs that can be upgraded concurrently is 10 (10 Mbps/1 Mbps). In addition, it is recommended that the maximum number of APs that can be concurrently upgraded by an AC be set to the number of upgrade groups multiplied by the number of APs that can be upgraded concurrently in a upgrade group, that is, 80.

3.3.4 Forwarding Data on the Tunnel

After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged over the data channel.

Working Principle

The CAPWAP sets up a control channel and a data channel between APs and ACs. The control channel is used by ACs to configure APs, or by APs to send event notifications to ACs, and must be encrypted. The data channel is used to exchange the 802.11 or 802.3 frames between APs and ACs. When running on the IPv4 protocol stack, the CAPWAP uses the UDP for data transmission. When running on the IPv6 protocol stack, the CAPWAP uses the UDP over the control channel, and UDP or UDP-lite over the data channel for data transmission.

3.4 Configuration

Configuration	Description and Command	
Configuring the AC Location	(Optional) It is used to configure the location information of an AC.	
	location	Configures the location information of an AC so that the physical location of the AC can be viewed.
Configuring the version number	(Optional) It is used to configure the version number.	
	set-version	Configures the version number,
Configuring the AP Location	(Optional) It is used to configure the location information of an AP.	
	location	Configures the location information of an AP so that the physical location of the AP can be viewed.
Configuring AP Time Synchronization	(Optional) It is used to enable the AP to synchronize the time with the AC.	
	timestamp	Enables the AP to synchronize the time with the AC.
Configuring Data to Allow an AP to Join an AC	(Optional) It is used to configure an AP on the AC to set up a CAPWAP tunnel.	
	ac-domain-name	Configures the DNS domain name of the AP, which is used to obtain the AC address.
	acip ipv4	Configures the static IP address of the AC accessed by the AP.
	acip ipv6	Configures the static IPv6 address of the AC accessed by the AP.
	ip address	Configures the static IP address, subnet mask, and gateway.
	ipv6 address	Configures the static IPv6 address and gateway.
	ipv6 enable	Enables the CAPWAP IPv6 function on the AP.
Configuring the ERPS ring	(Optional) It is used to configure the ERPS ring.	
	ap-cfg erps raps-vlan	Configures the EPRS ring.
Configuring an AP via an AC	(Optional) It is used to configure an AP via an AC.	
	exec-cmd	Executes ap-config commands on an AP/AP group via an AC.
Configuring a Fit AP	(Optional) It is used to perform pre-configuration on an AP to set up a CAPWAP tunnel.	
	acip ipv4	Configures the static IP address of the AC accessed by the AP.

	acip ipv6	Configures the static IPv6 address of the AC accessed by the AP.
	apip	Configures the static IP address, subnet mask, and gateway.
	apip ipv6 address	Configures the static IPv6 address and gateway.
	apip ipv6 address autoconfig default	Enables the AP to use the IPv6 stateless address autoconfiguration and generates a default route.
	apip ipv6 enable	Enables the IPv6 function of the AP.
	apip pppoe	Enables the AP to use the PPPoE dial-up mode to obtain the address.
Configuring AP Upgrade	(Optional) It is used to configure the AP upgrade data.	
	ap-serial	Creates the name of an AP product series, and specifies the AP product models that belong to this series.
	ap-image	In AP configuration mode, configures the specified AP upgrade version. In AC configuration mode, configures the specified AP software version that should be used by a specified AP product series for the upgrade, or sets the adaptive upgrade mode.
	active-bin-file	Activates the AP software version file.
	capwap upgrade max-concurrent	Configures the maximum number of APs that can be concurrently upgraded by the AC.
	capwap upgrade group	In AC configuration mode, creates a bandwidth control upgrade group.
	ap-upgrade band-width	In AC configuration mode, configures the bandwidth for centralized AP upgrade.
	ap-upgrade group	In AC configuration mode, adds APs to the bandwidth control upgrade group.
Configuring the CAPWAP Control Address	(Optional) It is used to configure the control IP address of the CAPWAP tunnel. When this address is not configured, the address of the loopback interface is used as the control IP address by default.	
	capwap ctrl-ip	Configures the control IP address of the CAPWAP tunnel.
Configuring CAPWAP Fragmentation	(Optional) It is used to configure CAPWAP fragmentation.	
	capwap mtu	Configures the maximum transmission unit (MTU) on the tunnel of a specified AP.
	capwap fragment enable	Enables CAPWAP fragmentation for a specified AP.

Configuring CAPWAP Encryption	(Optional) It is used to configure CAPWAP encryption.	
	capwap dtls enable	Enables encryption on the CAPWAP control channel.
Configuring CAPWAP Access Control	(Optional) It is used to control the maximum number of APs that can concurrently go online.	
	capwap max-concurrent	Configures the maximum number of APs that can concurrently go online.
Configuring the Echo Interval of the CAPWAP Tunnel	(Optional) It is used to configure the echo interval of the CAPWAP tunnel.	
	echo-interval	Configures the echo interval of the CAPWAP tunnel.
Configuring the Maximum Retransmission Times of a CAPWAP Packet	(Optional) It is used to configure the maximum transmission times of a CAPWAP packet.	
	capwap max-retransmit	Configures the maximum transmission times of a CAPWAP packet.

3.4.1 Configuring the AC Location

Configuration Effect

- Configure the location information of an AC so that users can conveniently check the locations of ACs on the WLAN.

Notes

- The location information is a string of 1 to 255 characters, and cannot contain any space.

Configuration Steps

- (Optional) Configure the AC location so that users can conveniently check the locations of ACs when a large number of ACs exist on the network.
- Enter the AC configuration mode, and run the **location** command to configure the AC location on the AC.
- Use the **no** form of this command to restore the default setting.

Command	**location** *location-string*
Parameter Description	*location-string*: indicates the location of an AC. The location is a string of 1 to 255 characters, and cannot contain any space.
Defaults	Ruijie_COM
Command Mode	AC configuration mode
Usage Guide	The AC location information is Ruijie_COM by default. You can configure the location information for each AC according to actual requirements so that you can conveniently check the AC location on the WLAN.

Verification

- Run the **show ac-config** command to display the AC location information and accordingly determine whether the configuration is successful.

Configuration Example

Configuring the AC Location Information as "computer-layer2"

Configuration Steps	• Enter the AC configuration mode. • Configure the AC location information.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)# locationcomputer-layer2`
	• Use the **no** form of this command to restore the default AC location information.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#no location`
Verification	Run the **show ac-config** command to display the current location of the AC.
AC	`Ruijie#show ac-config` `ac location :Ac_COM`

Common Errors

- N/A

3.4.2 Configuring the Version Number

Configuration Effect

- Customize the firmware version.

Notes

- The customized version number contains a maximum of 63 characters.

Configuration Steps

- Optional.
- Run this command to configure the customized firmware version number.
- Use the **no** form of this command to restore the default settings.

Command	**set-version** *string*

Parameter Description	*string*: indicates the customized version number.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the firmware version number of the AC and push the firmware version number to APs.

Verification

- Run the **show version** command to display the version number.

Configuration Example

Configuring the Customized Firmware Version Number to RGOS 10.4(2B17)-SP2

Configuration Steps	Enter the AC configuration mode. Configure the customized version number.
AC	`Ruijie(config)#ac-controller` `Ruijie(config-ac)# set-version RGOS 10.4(2B17)-SP2`
Verification	Run the **show version** command to display the version number.
AC	`Ruijie#show version` `System software version : RGOS 10.4(2B17)-SP2`

Common Errors

N/A

3.4.3 Configuring the AP Location

Configuration Effect

- Configure the location information of an AP.

Notes

- The AP location information is a string of 1 to 255 characters, and cannot contain any space.

Configuration Steps

Configuring the AP Location Information

- Optional.

- Run the **location** command to configure the AP location information.
- You can enter the AP configuration mode and configure the AP location information on the AC so that you can conveniently learn the physical location of the AP.

Command	**location***location-string*
Parameter Description	*location-string*: indicates the location of an AP. The location is a string of 1 to 255 characters, and cannot contain any space
Defaults	Null
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to display the AP location information.

Configuration Example

Configuring the Location Information of AP0001 as "AP-company"

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure the location information of AP0001 as "AP-company".
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# location AP-company`
Verification	• Run the **show ap-config running** command to display the location information of AP0001.
AC	`Ruijie#show ap-config running` `!` `ap-config AP0001` `location AP-company` `!`

Common Errors

- N/A

3.4.4 Configuring AP Time Synchronization

Configuration Effect

- Enable a specified AP or all APs in an AP group to synchronize the time with the AC.

Notes

- N/A

Configuration Steps

Enabling a Specified AP or All APs in an AP Group to Synchronize the Time with the AC

- Optional.
- To synchronize the time on the AP with that on AC, enter the AP or AP group configuration mode on the AC and run the **timestamp** command.

Command	timestamp
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Check whether the time on the AC is the same as that on the AP.

Configuration Example

Enabling AP0001 to Synchronize the Time with the AC

Configuration Steps	• Enter the AP configuration mode on the AC. • Enable AP0001 to synchronize the time with the AC.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# timestamp`
Verification	• Run the **show clock** command to display the time on the AP0001 and the AC.
AC	`Ruijie#showclock` `16:41:05 UTC Thu, Oct 17, 2013`

Common Errors

- N/A

3.4.5 Configuring Data to Allow an AP to Join an AC

Configuration Effect

- Configure the static IP addresses of ACs. The AP will send the Discover Request messages to these static IP addresses to check the effectiveness of ACs, and then select and joint an AC to set up a CAPWAP tunnel.

Notes

- A fit AP is generally not configured. It can discover ACs by means of broadcast, unicast, DHCP, or DNS, or join ACs based on the statically configured AC addresses.
- If the AP address is configured as the static address, the DHCP/DHCPv6 function will be disabled. In this case, the AC address cannot be obtained from the DHCP/DHCPv6 option. Therefore, before this command is configured, you need to configure the address of the connected AC in AP configuration mode so that the AP can discover and join the AC when the AP and the AC are not in the same subnet.
- If the current address of the AP is different from the address specified in the AC command, the AP static address will be updated and the CAPWAP tunnel will be re-established. If IPv6 is not enabled on the AP, the CAPWAP tunnel will not be re-established.
- If both the IPv4 and IPv6 addresses of the AP are specified in the configuration, and IPv6 is enabled on the AP, the AP will discover the IPv4 and IPv6 ACs simultaneously.

Configuration Steps

Configuring the Static AC Address

- Optional.
- The AC address can be obtained through DHCP or DNS. Alternatively, the static AC address can be configured in AP configuration mode on the AC or configured on the AP.
- When the AC address is obtained in static mode, run the **acip ipv4** or **acip ipv6** command to configure the static AC address.

Command	**acip ipv4***ip-address*[*ip-address*…]
Parameter Description	*ip-address*: indicates the static IP address. At most six static addresses can be configured.
Defaults	No static AC IP address is configured by default.
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Command	**acip ipv6** *ipv6-address*[*ipv6-address*…]
Parameter Description	*ipv6-address*: indicates the static IP address. At most six static addresses can be configured.
Defaults	N/A
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Configuring the Domain Name Used by the AP to Discover the AC

- (Optional) Run the **ac-domain-name** command to configure the DNS domain name on the AC so that the AP can discover the AC based on the DNS domain name.
- When the AC address is obtained in dynamic mode, configure the DNS domain name on the AC. The AC address can be obtained based on the DNS domain name.
- Generally, if the DNS domain name is not configured, the AP cannot obtain the IP address of the AC through the DNS.

Command	**ac-domain-name***ac-domain-name*
Parameter Description	*ac-domain-name*: indicates the AC domain name.
Defaults	ac.ruijie.com.cn
Command Mode	AP configuration mode or AP group configuration mode on the AC
Usage Guide	N/A

Configuring the Static IP Address of the AP

- Optional.
- On the AP, configure the static IPv4 or IPv6 address of the AP so that the AP can use the fixed IPv4 or IPv6 address to access the AC.

Command	**ip address** *ip-address network-mask gateway*
Parameter Description	*ip-address*: indicates the IP address of the AP. *network-mask*: indicates the subnet mask of the AP. *gateway*: indicates the gateway of the AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	An AP can obtain its own IP address through the static configuration or DHCP. If the static IP address is not configured on the AP, the AP obtains the address through DHCP and joins the AC. In this case, you can run this command to configure the static IP address of the AP so that the address can remain unchanged after the AP is restarted.

Configuring the Static IPv6 Address of a Specific AP

- Optional.

Command	**ipv6 address** *ipv6-address-with-mask gateway*
Parameter Description	*ipv6-address-with-mask*: indicates the IPv6 address of the AP. The format is X:X:X:X::X/24. *gateway*: indicates the IPv6 gateway of the AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	When IPv6 is enabled, the AP can obtain its own IPv6 address through the static configuration or DHCPv6. If the static IPv6 address is not configured on the AP, the AP obtains the address through DHCPv6 and

	joins the AC. In this case, you can run this command to configure the static IPv6 address of the AP so that the address can remain unchanged after the AP is restarted.

Enabling the AP to Support IPv6 Access

- Optional.
- Run this command to control whether an AP sets up a CAPWAP IPv6 tunnel.
- If a CAPWAP IPv6 tunnel needs to be set up, run the **ipv6 enable** command in AP configuration mode on the AC to support establishment of the IPv6 tunnel.

Command	**ipv6 enable**
Parameter Description	N/A
Defaults	IPv6 is disabled on the AP by default.
Command Mode	AP configuration mode
Usage Guide	If the IPv6 enable/disable status of the AP changes due to configuration of this command, the AP re-establishes the CAPWAP tunnel. When IPv6 is enabled on the AP, and the AP is configured with both static IPv4 and IPv6 addresses, the AP attempts to discover the IPv4 and IPv6 ACs simultaneously during re-establishment of the CAPWAP tunnel. For discovered ACs, the AP does not necessarily select and join an IPv6 AC. To ensure that the AP selects and joins an IPv6 AC, delete the IPv4 static address of the AP and retain only the static IPv6 address of the AP before IPv6 is enabled on the AP.

Verification

- Run the **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Enabling the AP to Obtain the IP Address of the AC Based on the Static IPv4 Address of the AP

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the static IP address of the AC accessed by the AP to 192.168.1.1. ● Set the static IP address of the AP to 1.1.1.1, subnet mask to 255.255.255.0, and gateway to 1.1.1.2.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# acip ipv4 192.168.1.1` `Ruijie(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2`
Verification	● Check the AP configurations.
AC	`Ruijie#show ap-config running` `!` `ap-config AP0001`

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the static IP address of the AC accessed by the AP to 192.168.1.1. ● Set the static IP address of the AP to 1.1.1.1, subnet mask to 255.255.255.0, and gateway to 1.1.1.2.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# acip ipv4 192.168.1.1` `Ruijie(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2`
Verification	● Check the AP configurations.
	`acip ipv4 192.168.1.1` `ip address 1.1.1.1 255.255.255.0 1.1.1.2` `!`

Enabling the AP to Obtain the IP Address of the AC based on the DNS Domain Name

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the DNS domain name of the AC to ruijie-ac.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# ac-domain-name ruijie-ac`
Verification	● Check the AP configurations.
AC	`Ruijie#show ap-config running` `!` `ap-config AP0001` ` ac-domain-name ruijie.ac` `!`

Enabling IPv6 on the AP

Configuration Steps	● Enter the AP configuration mode on the AC. ● Enable IPv6 on the AP.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# ipv6 enable`
Verification	● Check the AP configurations.
AC	`Ruijie#show ap-config running` `!` `ap-config AP0001`

Configuration Steps	● Enter the AP configuration mode on the AC. ● Enable IPv6 on the AP.
AC	`Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# ipv6 enable`
Verification	● Check the AP configurations.
	`ipv6 enable` `!`

Common Errors

- N/A

3.4.6 Configuring the ERPS Function on the AP

Configuration Effect

- The i-Share+ master AP requires the Ethernet Ring Protection Switching (ERPS) function. The fit AP does not save any configuration and therefore, the ERPS command needs to be saved.

Notes

- A link needs to be disconnected or a port needs to be shut down during network planning. The ring topology can be built only after the ERPS link is configured.
- Configure a Ring Protection Link (RPL) link on a device in the ERPS ring, so that traffic is balanced to dual upstream links. When one link fails or one device is faulty, the blocked RPL link is connected to prevent link failure.
- The VLAN used by the ERPS will occupy the VLAN capacity of the device. Therefore, the VLAN cannot be set to VLAN 1 or VLAN 2444, both of which are default VLANs. It cannot be the same with the VLAN of an STA specified by the **Interface-mapping** command or the VLAN of a wired port specified by the **wired-VLAN** command. It cannot be the same with the VLAN specified by the **ap-vlan** command, neither.

Configuration Steps

↘ Configuring an ERPS Single Ring

- Optional.
- Only the i-Share+ master AP supports this command.

Command	**ap-cfg erps raps-vlan** *vlan-id* **ring-port west** *interface-name1* **east** *interface-name2*
Parameter Description	*vlan-id*: indicates the R-APS VLAN ID. *interface-name1*: indicates the name of the west port. interface-name2: indicates the name of the east port.

Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**ap-cfg erps raps-vlan** *vlan-id* **rpl-port** { **west** | **east** } **rpl-owner**
Parameter Description	*vlan-id*: indicates the R-APS VLAN ID. **West**: specifies the west port to be the RPL owner. **east**: specifies the east port to be the RPL owner.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show erps** command to display the ERPS configuration.

Configuration Example

Configuring the ERPS Function on the AM5528

Configuration Steps	● Enter the AP configuration mode of the AC. ● Configure an ERPS single ring. ● Configure the RPL port.
AP	`Ruijie(config)#ap-cfg erps raps-vlan 10 ring-port west gigabitEthernet 0/26 east gigabitEthernet 0/25` `Ruijie(config)#ap-cfg erps raps-vlan 10 rpl-port east rpl-ower`
Verification	● Run the **show erps** command to display the ERPS configuration.
AP	`Ruijie(config)#show erps` `ERPS Information` `Global Status : Enabled` `Link monitored by : Not Oam` `----------` `R-APS VLAN : 10` `Ring Status : Enabled` `West Port : Gi0/26 (Link Failure)` `East Port : Gi0/25 (Forwarding)` `RPL Port : East Port` `Protected VLANs : ALL` `RPL Owner : Enabled` `Holdoff Time : 0 milliseconds` `Guard Time : 500 milliseconds` `WTR Time : 2 minutes` `Current Ring State : protection` `Associate R-APS VLAN :` `Ruijie(config)#`

Common Errors

- N/A

3.4.7 Configuring an AP to Execute a Command

Configuration Effect

- (Optional) On the AC, configure an AP to execute a command.
- (Optional) On the AC, configure all APs in an AP group to execute a command.

Notes

- N/A

Configuration Steps

Configuring an AP to Execute a Command

- (Optional) Enter the AP configuration mode.
- On the AC, configure the AP to execute a command.

Command	**exec-cmd mode** *exec-mode* **cmd** *exec-cmd* [**slot** { *id* | **all** } | **once**]
Parameter Description	*exec-mode*: indicates the mode in which a command is executed on the AP. *exec-cmd*: indicates the command to be executed on the AP. *id* : Indicates the slot ID of MAPs of i-Share+ AP. **all**: Indicates all MAPs of i-Share+ AP.**once**: indicates that the command is executed only once and is not saved.
Defaults	N/A
Command Mode	Single AP configuration mode/All APs configuration mode
Usage Guide	Some configuration commands are supported currently only by the AP and they are unavailable on the AC. To configure the commands for APs on the AC, run the **exec-cmd** command. To cancel or change the configuration of the **exec-cmd** command, run the **no exec-cmd** command to remove the configuration and then run the **exec-cmd** command to cancel or change the required configuration. Expanding the **exec-cmd** command delivers the command to MAP and run the command on the MAP. If **ap-config all** and **ap-config** are configured simultaneously, for online APs, the later configuration will take effect; for offline APs, **ap-config** has a higher priority than **ap-config all**. If the AC is already configured with a command for configuration delivery, please do not use this command again. Otherwise, the configuration may conflict. Note: If a dedicated command is used on an AC to deliver configurations to an AP, do not use this command to deliver the configurations. Otherwise, conflicts occur.

Verification

- Log in to the AP to check whether the configuration takes effect. On the AC, run the **show run** or **show ap-config run** command to check whether the configuration takes effect.

Configuring APs in an AP Group to Execute a Command

- (Optional) Enter the AP group configuration mode.
- Configure all APs in an AP group to execute a command.

Command	**exec-cmd** *exec-cmd*
Parameter Description	*exec-cmd*: indicates the command to be executed on all APs in an AP group.
Defaults	N/A
Command Mode	AP group configuration mode.
Usage Guide	Some configuration commands are available only in AP configuration mode and they are unavailable in AP group configuration mode. To configure such a command for all APs in an AP group, run the **exec-cmd** command in the AP group. Note that the configuration is not saved in AP group configuration mode, that is, the command is executed only once on all APs in the current AP group. If the configuration already exists in AP configuration mode, the original configuration will be overridden when the command is executed in AP group configuration mode. Note: If a dedicated command is used on an AC to deliver configurations to an AP, do not use this command to deliver the configurations. Otherwise, conflicts occur.

Verification

- Run the **show ap-config run** command to check whether the configuration of the APs in an AP group takes effect.

Configuration Example

Disabling the Eweb Function for an AP on the AC and Configuring Bluetooth iBeacon for all APs in an AP Group

Configuration Steps	● On the AC, disable the Eweb function for APs. ● On the AC, enable the Eweb function for APs. ● Enable Bluetooth iBeacon for all APs in an AP group. ● Disable the Eweb function for all APs in the AP group.
AC	`Ruijie(config)#ap-config AP1` `Ruijie(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"` `Ruijie(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all"` `Ruijie(config-ap)# exec-cmd mode configure cmd "enable service web-server all"` `Ruijie(config)#ap-group default` `Ruijie(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff` `Ruijie(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"`
Verification	● On the AC, check whether the configuration takes effect.
AC	`Ruijie#show ap-config running` `ap-config AP1` `exec-cmd mode configure cmd "no enable service web-server all"` `ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff`

Common Errors

The **exec-cmd** command needs to be changed, but the **no exec-cmd** command is not executed to delete original configuration, or the **exec-cmd** command is not re-executed to cancel the configuration.

3.4.8 Configuring a Fit AP

Configuration Effect

- Configure the static IP address, subnet mask, next hop, and AC address on a fit AP so that the AP can use the static address to communicate with the AC.

Notes

- If the AP address is configured as the static address, the DHCP function will be disabled. In this case, the AC address cannot be obtained from the DHCP/DHCPv6 option. Therefore, you need to configure the address of the connected AC on the fit AP so that the AP can discover and join the AC when the AP and the AC are not in the same subnet.
- The fit AP configuration commands have the same functions as some AP configuration commands used on the AC. When the two configurations conflict with each other, the AP may be re-connected to the AC only based on the configurations on the AC.
- The fit AP configuration commands are automatically saved.

Configuration Steps

Configuring the Static IP Address of the AP

- Optional.
- When IP addresses of APs must be statically planned at the early stage of deployment, you can configure IP addresses on the APs.
- Configure the static IPv4 or IPv6 address of the AP so that the AP can use the IPv4 or IPv6 address to access the AC.
- Run the **apip ipv4** command to configure the static IPv4 address of the AP.
- Run the **apip ipv6** command to configure the static IPv6 address of the AP.

Command	**apip ipv4** *ip-addressnetwork-mask gateway*
Parameter Description	*ip-address*: indicates the static IP address. *network-mask*: indicates the subnet mask. *gateway*: indicates the gateway address.
Defaults	N/A
Command Mode	Global configuration mode on the AP
Usage Guide	N/A

Command	**apip ipv6** *ipv6-address-with-mask gateway*
Parameter Description	*ipv6-address-with-mask*: indicates the IPv6 address containing the mask length. The format is X:X:X:X::X/24. *gateway*: indicates the IPv6 gateway address.
Defaults	N/A
Command Mode	Global configuration mode on the AP
Usage Guide	N/A

Configuring the Static IP Address of the AC Accessed by the AP

- Optional.

- When the AP is configured to use the static IP address, you must also specify the IP address of the accessed AC on the AP.
- The static address type of the AC accessed by the AP must be the same as that of the AP. Ensure that both the AC and the AP use the IPv4 static address, or both use the IPv6 static address.
- Run the **acip ipv4** command so that the AP joins a specified IPv4 AC.
- Run the **acip ipv6** command so that the AP joins a specified IPv6 AC.

Command	**acipipv4** *ip-address*[*ip-address*…]
Parameter Description	*ip-address*: indicates the static IP address. At most six static addresses can be configured.
Defaults	N/A
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Command	**acipipv6** ipv6-address [*ipv6-address*…]
Parameter Description	*ipv6-address*: indicates the IPv6 address of the connected AC. At most six static addresses can be configured.
Defaults	N/A
Command Mode	Global configuration mode on the AP or AP configuration mode on the AC
Usage Guide	N/A

Enabling the AP to Use the Stateless Address

- Optional.
- On the AP, configure data so that the AP uses the IPv6 stateless address autoconfiguration and a default route is generated.
- Run the **apip ipv6 enable** command to enable the IPv6 function of the AP.

Command	**apip ipv6 address autoconfig default**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode on the AP
Usage Guide	After this command is executed, the AP uses the IPv6 stateless address autoconfiguration, and a default route is generated.

Command	**apip ipv6 enable**

Parameter Description	N/A
Defaults	The IPv6 function of the AP is enabled by default.
Command Mode	Global configuration mode on the AP
Usage Guide	You can run this command to enable or disable the CAPWAP IPv6 discovery function only on an IPv4 network.

Configuring the CAPWAP IPv6 Discovery Function on the AP

- Optional.
- You can disable the CAPWAP IPv6 discovery function only on an IPv4 network to prevent the attempts made by CAPWAP to set up an IPv6 tunnel, thus reducing the CAPWAP packets on the network.
- Run the **no apip ipv6 enable** command to disable the IPv6 function of the AP.

Command	**apip ipv6 enable**
Parameter Description	N/A
Defaults	The IPv6 function of the AP is enabled by default.
Command Mode	Global configuration mode on the AP
Usage Guide	You can run this command to enable or disable the CAPWAP IPv6 discovery function only on an IPv4 network.

Enabling the AP to Use the PPPoE Dial-up Mode to obtain the Address

- Optional.
- When the AP needs to connect to a remote Internet service provider (ISP) through the ADSL and obtains the network access capability, run this command so that the AP can use the PPPoE dial-up mode to obtain the address.

Command	**apip pppoe**
Parameter Description	N/A
Defaults	By default, the PPPoE mode is not specified and the AP obtains the address through DHCP.
Command Mode	Global configuration mode on the AP
Usage Guide	The command configures only the mode (PPPoE dial-up mode) selected by the AP to obtain the address. After this command is configured, you need to add the PPPoE configurations and let the default route to point to the dialer interface so that the AP can communicate with the AC. CAPWAP can only select dialer 1 as the source interface. Therefore, when configuring the PPPoE dial-up mode, dialer 1 must be used.

Verification

- Check whether the fit AP configuration commands exist.
- Check whether the AP can communicate with the AC.

Configuration Example

Configuring the Static IP Address of the AC Accessed by the AP

Configuration Steps	● Configure the static IPv4 address of the AP. ● Configure the static IPv4 address of the AC accessed by the AP.
AP	`Ruijie(config)# apip 192.168.1.2 255.255.255.0 192.168.1.1` `Ruijie(config)# acip ipv4 1.1.1.1`
Verification	● Run the **show running-config** command to display the configurations.
AP	`!` `apip 192.168.1.2 255.255.255.0 192.168.1.1` `acip ipv4 1.1.1.1` `!`

Enabling the AP to Use the PPPoE Dial-up Mode to Obtain the Address

Configuration Steps	● Enable the AP to select the PPPoE dial-up mode to obtain the address. ● Configure the PPPoE. ● Configure the default route. ● Configure the static IPv4 address of the AC accessed by the AP.
AP	`Ruijie(config)# apip pppoe` `Ruijie(config)# interface FastEthernet 0/1` `Ruijie(config-if-FastEthernet 0/1)#pppoe enable` `Ruijie(config-if-FastEthernet 0/1)#pppoe-client dial-pool-number 1 no-ddr` `Ruijie(config-if-FastEthernet 0/1)#exit` `Ruijie(config)# interfacedialer 1` `Ruijie(config-if-Dialer1)#ip address negotiate` `Ruijie(config-if-Dialer1)#ppp chap hostname ruijie` `Ruijie(config-if-Dialer1)#ppp chap password ruijie` `Ruijie(config-if-Dialer1)#ppp pap sent-username ruijie password ruijie` `Ruijie(config-if-Dialer1)#dialer pool 1` `Ruijie(config-if-Dialer1)#exit` `Ruijie(config)#ip route 0.0.0.0 0.0.0.0 dialer 1` `Ruijie(config)# acip ipv4 1.1.1.1`
Verification	● Run the **show running-config** command to display the configurations.
AP	`!` `apip 192.168.1.2 255.255.255.0 192.168.1.1` `acip ipv4 1.1.1.1` `!`

Common Errors

- N/A

3.4.9 Configuring AP Upgrade

Configuration Effect

- Upgrade the AP software version through configuration on the AC.

Notes

- Configure the data to activate the AP software version file. This command loads the **.bin** file to the memory only when the AP needs to be upgraded. When no AP needs to be upgraded, the bin file will be automatically removed from the memory.

- During the adaptive upgrade, the transitional version between rgos10 and rgos11 cannot be used to upgrade an AP using the rgos10 system.
- When the bandwidth is limited, use the bandwidth control function for the upgrade.

Configuration Steps

Creating the AP Product Series

- (Optional) Run the **ap-serial** command to configure an AP product series on the AC.
- To upgrade the AP software version through the AC, you must configure the AP hardware version and product models for a specified product series on the AC.
- An AP software version is applicable to a series of AP products. You can configure the AP hardware version and product models for a specified product series, and use the software version to upgrade specified AP models.

Command	**ap-serial***serial-name ap-pid1 ap-pid2 ... ap-pidn* [**hw-ver** *hardware-version*]
Parameter Description	*serial-name*: indicates the name of the AP series to be created. *ap-pid1 ap-pid2 ... ap-pidn*: lists the product models to be added to the AP series. *hardware-version*: specifies the AP hardware version.
Defaults	No AP series is configured by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Activating the AP Software Version File

- (Optional) Run the **active-bin-file** command to activate an AP software version on the AC.
- To upgrade the AP software version through the AC, you must activate the AP software version on the AC.
- Only an activated AP software version can be used for the upgrade.

Command	**active-bin-file** *filename*[**rgos10**]
Parameter Description	*filename*: specifies the name of a software version. The name may contain a path prefix (**flash:**,**tmp:**, or**usb0:**), followed by a real file name. The maximum length of a file name is 64 bytes. **rgos10:** indicates that a transitional version between 10.X and 11.X is activated. It is applicable only to the AP software version.
Defaults	The AP software version is not activated by default.
Command Mode	AC configuration mode
Usage Guide	1. To download a software version from the AC to upgrade an AP, you must first activate the version file. The rgos10 system differs a lot from the rgos11 system. Therefore, when using a transitional version between rgos10 and rgos11 for the upgrade, you must add the rgos10 keyword. 2. The **.bin** file is loaded to the memory only when an AP needs to be upgraded. When no AP needs to be upgraded, the bin file will be automatically removed from the memory.

	3. Before configuring this command, ensure that the software version file already exists in the AC system files.

Upgrading the Version of Specified APs

- Optional: Run the **ap-image** command to use a specified file to upgrade a specified AP series on the AC. This command takes effect on all APs connected to the AC.
- To upgrade the AP software version through the AC, you must first specify the upgrade file used by the AP.
- To upgrade a specified AP series, you must activate the AP software version, specify the AP series, and specify a file for upgrading the specified AP series.

Command	**ap-image** *filename*
Parameter Description	*filename*: specifies the software version name.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Adaptive Upgrade

- (Optional) Run the **ap-image auto-upgrade** command so that the AC can automatically identify applicable AP products based on the AP upgrade file and upgrade all applicable APs.
- The command automatically matches the AP models to which the software version is applicable and upgrades these APs.

Command	**ap-image**{ **auto-upgrade** | *filename serial-name*}
Parameter Description	**auto-upgrade:** indicates that the product model is automatically matched for the upgrade. *filename*: specifies the software version name. This file name must be the same as that specified by the **active-bin-file** command. *serial-name*: indicates the name of the AP series to be upgraded.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	You can use the **auto-upgrade** option to automatically match the software version and upgrade APs without configuring the mapping relationship between the AP product models and software version. You can also use a specified file to upgrade a specified AP product series. When both the automatic upgrade mode and the specified series upgrade mode exist, the specified series upgrade mode is used preferentially. To enable the AC to upgrade the version of a specified AP product series, you must create the AP product series, configure the software version corresponding to the specified APs, and activate the software version. The three steps are mandatory.

Configuring AP Upgrade Function in Hierarchical AC Scenarios

- Optional.

- Enable the AP upgrade function on the center AC or a branch AC in hierarchical AC scenarios.

Command	**capwap upgrade center enable**
Parameter Description	N/A
Defaults	The AP upgrade function is enabled on the center AC by default (disabled on branch ACs).
Command Mode	AC configuration mode
Usage Guide	1. This command applies only to hierarchical AC scenarios. 2. When the AP upgrade function on an AC is changed from enabled to disabled, upgrade configurations (activated bin, automatic upgrade, sequential upgrade, and single AP upgrade) on the AC are automatically cleared. 3. After a branch AC connects to the center AC, the branch AC automatically synchronizes configurations of the center AC. 4. When a branch AC is in the connected state, configurations on the branch AC cannot be modified. The configurations can only be modified on the center AC and automatically synchronized to the branch AC. When the branch AC is in the standalone state, configurations on the branch AC can be modified.

Configuring the Maximum Number of APs That Can Be Concurrently Upgraded by the AC

- Optional.
- Limit the maximum number of APs that can be concurrently upgraded by the AC.

Command	**capwapupgrade max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can be concurrently upgraded by the AC. The default value is 18. The value ranges from 1 to 200.
Defaults	15
Command Mode	AC configuration mode
Usage Guide	N/A

Creating an Upgrade Group

- Optional.
- Create an upgrade group. The AC can evenly distribute the centralized upgrade quota to the upgrade group through balanced scheduling to limit the bandwidth and avoid wasting the bandwidth.

Command	**capwap upgrade group** *group-name* [**max-concurrent***num*]
Parameter Description	*group-name*: indicates the name of an upgrade group. The upgrade group name cannot be set to "default". *num*: indicates maximum number of APs that can be concurrently upgraded in the group. The default value is 5. The value ranges from 1 to 200.
Defaults	By default, no upgrade group is configured, and the AP upgrade is not limited by the bandwidth. When configuring an upgrade group, the maximum number of APs that can be concurrently upgraded in the group is 5 by default.

Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an Upgrade Group

- Optional.
- Add APs to an upgrade group. Limit the number of APs that are upgraded in a centralized manner in this group through scheduling and configuration to control the bandwidth by upgrade group.

Command	**ap-upgrade group** *group-name*
Parameter Description	*group-name*: indicates the name of the upgrade group. Before adding APs to an upgrade group, you must run the **capwap upgrade group** command to create the upgrade group.
Defaults	APs are not added to any upgrade group.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Bandwidth Used for AP Upgrade

- Optional.
- Configure the bandwidth used for AP upgrade.

Command	**ap-upgrade band-width***num*
Parameter Description	*num*: indicates the bandwidth used for AP upgrade. The unit is 1 KB. The value ranges from 8 to 1024.
Defaults	The bandwidth is not limited.
Command Mode	AP configuration mode
Usage Guide	The bandwidth-limited AP upgrade configuration commands include the command for configuring the bandwidth used for AP upgrade, the command for creating an upgrade group, and the command for adding APs to the upgrade group.

Verification

- Check whether the AP version is successfully upgraded.
- Check the upgrade status of the bandwidth control upgrade group and APs in the group.

Configuration Example

Configuring the AP Upgrade Data

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create the name of an AP product series on the AC. ● Activate the specified AP software version used for the upgrade on the AC. ● Configure the AP upgrade version file on the AC.
AC	`Ruijie(config-ac)# ap-serial serial1 AP220-E AP220-SE AP620-H hw-ver 1.0` `Ruijie(config-ac)# active-bin-file ap.bin` `Ruijie(config-ac)# ap-image ap.bin serial1` `Ruijie(config-ac)# exit`
Verification	● Display the list of files activated on the AC.
AC	`Ruijie#show ac-config active-file` `Cnt File Name Version Used Cnt Ready` `------ ------------ ---------- ---------- --------` `1 ap.bin RGOS 10.4(1t7)(1T7), Release(88888) 1 1`

Configuring the AP Upgrade During Which the Bandwidth is Under Control

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create an AP upgrade group on the AC. ● Exit from the AC configuration mode. ● Enter the AP configuration mode. ● Configure the specified AP upgrade group on the AC. ● Activate the bandwidth used for AP upgrade on the AC.
AC	Ruijie(config-ac)# capwap upgrade group UPGRADE-GROUP1 max-concurrent 10 Ruijie(config-ac)# exit Ruijie(config)#ap-config 8832.0000.1111 Ruijie(config-ap)# ap-upgrade group UPGRADE-GROUP1 Ruijie(config-ap)# ap-upgrade band-width 128 Ruijie(config-ap)# exit
Verification	● Display the upgrade group and APs in the group on the AC. ● Display the APs and their bandwidths in an upgrade group on the AC.
AC	Ruijie#show ac-config upgrade-group Cnt Group-Name Max-Concurrent Token cnt Upgrading cnt ------ ---------- ---------- ---------- 1 UPGRADE-GROUP1 10 2 1 Ruijie#show ac-config upgrade-groupUPGRADE-GROUP1 Group have 2 ap, online 1 offline 1 Cnt Ap-Name Ap-Mac Online Upgrade Band-width ------- ---------- ---------- ------- --------- 1 ap220e 8832.0000.1111 true true 128 2 ap330 - false false 128 Ruijie#show ap-config wtp-info 8832.0000.1111 Ruijie#show ap-config wtp-info ap220e Upgrade-banfwidth : 128 Upgrade group : UPGRADE-GROUP1

Configuring AP Upgrade Function in Hierarchical AC Scenarios

Configuration Steps	1. Enable the AP upgrade function on the center AC (and disable it on branch ACs). `Ruijie(config-ac)# capwap upgrade center enable` 2. Enable the AP upgrade function on a branch AC (and disable it on the center AC). `Ruijie(config-ac)# no capwap upgrade center enable` 3. Cancel the configurations. `Ruijie(config-ac)# default capwap upgrade center enable`
Verification	Run the **show running-config** command to check whether the configuration is successful.

Common Errors

- The AP upgrade data is configured, but the software version file used for the upgrade does not exist in the AC system files.

3.4.10 Configuring a Mini AP

Configuration Effect

- One rack-type AP can carry multiple mini APs. This operation is performed to manage and name mini APs, and display their installation status, thus facilitating the mini AP management.

Notes

- N/A

Configuration Steps

↘ Naming a Mini AP

- (Optional) Run the **slot** command to name a mini AP in a specified slot.
- This configuration takes effect only for i-Share APs. The corresponding radio frequency (RF) card can be named to determine the position of this card.

Command	**slot** *slot-id* {*slot-name* [**secondary**] | **mac** *mac-address slot-name* }
Parameter Description	*slot-id*: indicates the slot ID. The slot ID ranges from 1 to 24. *slot-name*: indicates the name of an AP card. The name is a string of 1 to 63 characters, and cannot contain any space. **secondary**: Applies to the secondary AP. *mac-address*: MAC address of the Mini AP.
Defaults	An AP card is not named by default.

Command Mode	AP configuration mode
Usage Guide	This command takes effect only for i-Share+ APs and cannot be configured for all APs. If you want to name a secondary Mini AP, please add the **secondary** parameter. Each slot can be configured with two MAC addresses.

Updating the Installation Status of Mini APs

- (Optional) Run the **install update** or **uninstall** command to update the installation status of mini APs.
- If the state of a removed mini AP is displayed as offline, you can update its installation status.

Command	**install update**
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	If a mini AP is installed in a specified slot on the rack-type AP but is later manually removed, the system determines that this mini AP is offline. This command is executed to query a rack-type AP that is currently online, and the online mini APs on the rack are treated as installed mini APs. Configurations of this command are not saved.

Command	**uninstall** *slot-id* [**secondary**]
Parameter Description	*slot-id*: indicates the slot ID. The slot ID ranges from 1 to 24. **secondary**: Applies to the secondary AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	If a mini AP is installed in a specified slot on the rack-type AP but is later manually removed, the system determines that this mini AP is offline. You can use this command to remove a mini AP from the corresponding slot. If the mini AP in this slot is online, execution of this command is meaningless. Configurations of this command are not saved. In addition, the command cannot be used in all AP configuration mode. If you want to name a secondary Mini AP, please add the **secondary** parameter.

Restarting a Mini AP

- (Optional) Run the **reset slot** *slot-id* command to restart a mini AP in a specified slot.
- To reset a mini AP, you can use this command to power off the mini AP and then power it on again.
- This command applies to two Mini APs of a slot.

Command	**reset slot** *slot-id*
Parameter Description	*slot-id*: indicates the slot ID. The slot ID ranges from 1 to 24.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	This command takes effect only on a rack-type AP, and cannot be used in all AP configuration mode. Configurations of this command are not saved.

Verification

- Check the installation information of mini APs, including the names and online status.

Configuration Example

Naming a Mini AP

Configuration Steps	● Enter the AP configuration mode on the AC. ● Name the mini AP in a specified slot.
AC	The following example sets the name of Mini AP1 to 1#101. `Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# slot 1 Dormitory 1#101` The following example sets the name of AP0001, secondary Mini AP1 of slot 1, to 1#102. `Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# slot 1 1#102 secondary` The following example sets the name of Mini AP (MAC address: 0001.0001.0001) of slot 1 to 1#101 and the name of Mini AP (MAC address: 0001.0001.0002) of slot 1 to 1#102. `Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# slot 1 mac 0001.0001.0001 1#101` `Ruijie(config-ap)# slot 1 mac 0001.0001.0002 1#102`
Verification	● Check the name of the mini AP on the AC.
AC	`Ruijie#show ap-config summary slot` `Total Install Number: 2` `Total Online Number: 1` `Total Offline Number: 1` `AP(AP0001)'s Slots Information` `Install Number: 2` `Online Number: 1` `Offline Number: 1` `AP mac Slot ID Role Slot Name Model Slot Mac Radio Radio Up/Off time State` `-------------- ------- --------- ------------------------------ --------- -------------- - ------------------- ------------------- ----------- -------` `00d0.f822.3418 1 master Dormitory 1#101 MAP552 5869.6c36.e268 1 E 0 6* 100 2 E 0 157* 100 1:03:39:38 online` `00d0.f822.3418 2 slave Dormitory 1#102 MAP552 5869.6c36.e269 3 N 4 N 1:03:39:38 offline`

Common Errors

- N/A

3.4.11 Configuring the CAPWAP Address Control

Configuration Effect

- Configure the maximum number of APs that can concurrently go online.

Notes

- If the configured value is too small, the total online duration of all APs connected to the AC will be relatively long.

Configuration Steps

↘ Configuring the Maximum Number of APs That Can Concurrently Go Online

- Optional.
- On the AC, configure the maximum number of APs that can concurrently go online to prevent an excessively high CPU usage caused by a large number of CAPWAP control packets.

Command	**capwap max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can concurrently go online. The number ranges from 1 to 200.
Defaults	50
Command Mode	AC configuration mode
Usage Guide	If a large number of APs go online concurrently, the CPU usage of the AC may increase or even reach 100%. Consequently, tunnels of APs that are already online will be disconnected due to keepalive failures. You can use this command to limit the maximum number of APs go online concurrently.

↘ Configuring the Number of CAPWAP Discovery Packets That Can Be Processed by an AC

- Optional.
- Configure the maximum number of discovery packets that can be processed by an AC on the AC to prevent exceedingly high CPU usage caused by considerable CAPWAP control packets.
- Run the ***capwap disc-concurrent*** *num* command to configure the number of discovery packets that can be processed.

Command	**capwap disc-concurrent** *num*
Parameter Description	The number of discovery packets that can be processed per second depends on the product capacity.
Defaults	The default value varies with the capacity value, for example, the default value is **256** for the WS7800.
Command Mode	AC global configuration mode

Usage Guide	The CAPWAP module needs to restrict the discovery packet processing concurrency based on the AC capacity, to prevent discovery packet attacks.

Verification

- Run the **show running-config** command to display the configurations.

Configuration Example

↘ Configuring the Maximum Number of APs That Can Concurrently Go Online

Configuration Steps	● On the AC, configure the maximum number of APs that can concurrently go online.
AC	`Ruijie(config-ac)#capwap max-concurrent 100`
Verification	● On the AC, run the **show running-config** command to display the configurations.
AC	`!` `ac-controller` `capwap max-concurrent 100` `!`

Common Errors

- N/A

3.4.12 Configuring CAPWAP Fragmentation

Configuration Effect

- After a packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the packet may be fragmented and reassembled for several times, which reduces the packet forwarding performance. After CAPWAP fragmentation is enabled, the packet will be fragmented when encapsulated on the CAPWAP channel. The CAPWAP packet length is specified as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Notes

- If the configured MTU is too small, a lot of fragmented packets will be generated, affecting the packet forwarding performance. Even worse, large packets may fail to be transmitted. Therefore, it is important to determine the size of the MTU.
- The configured CAPWAP MTU must be equal to or smaller than the IP MTU at the egress of the device; otherwise, IP fragmentation will be performed after CAPWAP fragment. The minimum IPv6 MTU is 1280, that is, the minimum path MTU is 1280. Therefore, the CAPWAP MTU must be equal to or greater than 1280.

Configuration Steps

Configuring the Path MTU of the CAPWAP Tunnel

- (Optional) Enter the AP or AP group configuration mode, and run the **capwap mtu** command to configure the path MTU of the CAPWAP tunnel.
- If the length of the packet encapsulated on the CAPWAP tunnel exceeds the path MTU of the CAPWAP tunnel, the packet will be fragmented on the CAPWAP tunnel. When configuring the path MTU of the CAPWAP tunnel on the AC, this path MTU must be set to the minimum IP MTU on the tunnel; otherwise, IP fragmentation and reassembly are performed again during packet forwarding, reducing the forwarding performance.

Command	**capwap mtu** *num*
Parameter Description	*num*: indicates the path MTU of the CAPWAP tunnel. The value ranges from 68 to 1500. The unit is byte.
Defaults	The default size of the MTU is 1500 bytes.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Enabling CAPWAP Fragmentation

- Optional.
- When multiple IP MTU nodes exist on the transmission network, it is recommended that CAPWAP fragmentation be enabled on the AC, and the CAPWAP MTU be set to the path MTU.
- After a packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the packet may be fragmented and reassembled for several times, which reduces the packet forwarding performance. You can run this command to enable CAPWAP fragmentation. After this function is enabled, the packet will be fragmented when encapsulated on the CAPWAP channel. The CAPWAP packet length can be specified in the **capwap mtu** command as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Command	**capwap fragment enable**
Parameter Description	N/A
Defaults	CAPWAP fragmentation is disabled by default.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Check the detailed information about the CAPWAP to learn the MTU of the CAPWAP tunnel and whether the fragmentation function is enabled.
- Alternatively, run the **show ap-config running** command to check whether CAPWAP fragmentation is configured.

Configuration Example

Configuring the MTU of AP1 and Enabling the Fragmentation Function

Configuration Steps	● Set the path MTU of AP1 to 1200 bytes on the AC. ● Enable CAPWAP fragmentation of AP1 on the AC.
AC	`Ruijie(config)# ap-config AP1` `Ruijie(config-ap)# capwap mtu 1200` `Ruijie(config-ap)# capwap fragment enable`
Verification	Use the **show ap-config running** command to display the configurations.
AC	`!` `capwap fragment enable` `capwap mtu 1200` `!`

Common Errors

- N/A

3.4.13 Configuring CAPWAP Encryption

Configuration Effect

- Disable the encryption function on the CAPWAP control channel to analyze packets when the network is faulty.

Notes

N/A

Configuration Steps

Configuring the Encryption Function on the CAPWAP Control Channel

- Optional.
- On the AC, you can disable the encryption function on the CAPWAP control channel to analyze packets for troubleshooting purpose when the network is faulty.

Command	**capwap dtls enable**
Parameter Description	N/A
Defaults	By default, the DTLS encryption function is enabled on the CAPWAP control channel.
Command Mode	AC configuration mode

Usage Guide	By default, the DTLS encryption function is enabled on the CAPWAP control channel to ensure security of interaction between the AC and the AP. In special cases, you can disable the encryption function on the CAPWAP control channel to facilitate tests.

Verification

- Check the detailed information about the CAPWAP tunnel to determine the encryption policy of the control channel and the data channel.
- Run the **show running-config** command to check whether encryption is enabled on the control channel.

Configuration Example

↘ Enabling Encryption on the AP Data Channel and Disabling Encryption on the Control Channel

Configuration Steps	● On the AC, disable the encryption function on the AP control channel.
AC	`Ruijie(config-ap)# no capwap dtls enable`
Verification	● On the AC, run the **show running-config** command to check whether the encryption function is disabled on the control channel.
AC	`Ruijie#show running-config` `!` `no capwap dtls enable`

Common Errors

- N/A

3.4.14 Configuring CAPWAP Access Control

Configuration Effect

- Configure the maximum number of APs that can concurrently go online.

Notes

- If the configured value is too small, the total online duration of all APs connected to the AC will be relatively long.

Configuration Steps

↘ Configuring the Maximum Number of APs That Can Concurrently Go Online

- Optional.
- On the AC, configure the maximum number of APs that can concurrently go online to prevent an excessively high CPU usage caused by a large number of CAPWAP control packets.

Command	**capwap max-concurrent** *num*
Parameter Description	*num*: indicates the maximum number of APs that can concurrently go online. The number ranges from 1 to 200.
Defaults	50
Command Mode	AC configuration mode
Usage Guide	If a large number of APs go online concurrently, the CPU usage of the AC may increase or even reach 100%. Consequently, tunnels of APs that are already online will be disconnected due to keepalive failures. You can use this command to limit the maximum number of APs go online concurrently.

Verification

- Run the **show running-config** command to display the configurations.

Configuration Example

↘ Configuring the Maximum Number of APs That Can Concurrently Go Online

Configuration Steps	• On the AC, configure the maximum number of APs that can concurrently go online.
AC	`Ruijie(config-ac)#capwap max-concurrent 100`
Verification	• On the AC, run the **show running-config** command to display the configurations.
AC	`!` `ac-controller` `capwap max-concurrent 100` `!`

Common Errors

- N/A

3.4.15 Configuring the Echo Interval of the CAPWAP Tunnel

Configuration Effect

- (Optional) Configure the interval at which a keepalive packet is set.

Notes

- During deployment of the wireless network, the echo interval of the CAPWAP tunnel can be adjusted according to the network scale to properly plan the network convergence performance. During the adjustment, ensure that you have a good understanding about the network scale and confirm that the convergence is necessary. If a low echo interval is configured on a wireless network where a large number of APs are deployed, the network environment will be affected.

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode for configuration.
- Configure the echo interval of the CAPWAP tunnel on the AC to control the keepalive period of the CAPWAP tunnel.

Command	**echo-interval** *seconds*
Parameter Description	*seconds*: indicates the echo interval of the CAPWAP tunnel. The value ranges from 5 to 255.
Defaults	30s
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	In a fit AP network structure, an AC is interconnected with an AP through the CAPWAP tunnel. The Echo Request and Echo Response packets are used between the AP and the AC to maintain the effectiveness of links. If other request packets are not transmitted, the AP sends an Echo Request packet to the AC at the interval specified by **echo-interval** to keep the CAPWAP tunnel alive. If the AP does not receive any Echo Response packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit (**the maximum retransmission times) is reached, it is determined that the CAPWAP tunnel is disconnected. That is, the keepalive failure time of the tunnel is equal to the keepalive time plus the retransmission interval. This command takes effect only when the tunnel is in Run state. By default, **echo-interval** is 30s, and **max-retransmit** is 5. If the Echo Response packet is not received 0s after the Echo Request packet is sent, the Echo Request packet will be retransmitted at the interval of 3s, 6s, 12s, 15s, and 15s, respectively. The same rule is observed to calculate the packet timeout time if **echo-interval** and **max-retransmit** are set to other values.

Verification

- Check the detailed information about the CAPWAP tunnel. The modified interval at which the keepalive packet is sent should be displayed.

Configuration Example

↘ Configuring the Echo Interval of the CAPWAP Tunnel

Configuration Steps	● On the AC, set the echo interval of the CAPWAP tunnel to 50s.
AC	`Ruijie(config)#ap-config AP0001` `Ruijie(config-ap)# echo-interval 50`
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.
AC	`Ruijie#show capwap 1.1.1.1 detail` `Echo interval is 50 secs, Dead interval is 119 secs`

Common Errors

- N/A

3.4.16 Configuring the Maximum Retransmission Times of a CAPWAP Packet

Configuration Effect

- (Optional) Configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel.

Notes

N/A

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode for configuration.
- Configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel.

Command	**capwap max-retransmit***num*
Parameter Description	*num*: indicates the maximum retransmission times of a CAPWAP packet
Defaults	5
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	If the AP does not receive any Echo Response packet after sending an Echo Request packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit (**the maximum retransmission times) is reached, it is determined that the CAPWAP tunnel is disconnected. You can configure the maximum transmission times of a CAPWAP packet to adjust the keepalive time of the CAPWAP tunnel. This command takes effect only when the tunnel is in Run state.

Verification

- Check the detailed information about the CAPWAP tunnel. The modified interval at which the keepalive packet is sent should be displayed.

Configuration Example

Configuring the Maximum Retransmission Times of a CAPWAP Packet

Configuration Steps	● Set the maximum retransmission times of AP1 to 20.
AC	`Ruijie(config)#ap-config AP1` `Ruijie(config-ap)# capwap max-retransmit 20`
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.
AC	`Ruijie#show capwap 1.1.1.1 detail` `Config maxretransmit 20`

Common Errors

- N/A

3.4.17 Configuring the AC Discovery Mode

Configuration Effect

- An AP can send discovery packets of a recommended type, DHCP packets, DNS packets, packets carrying the statically configured AC IP address, and packets of other types (for example, broadcast and multicast packets) to an AC. An AC can be configured to respond only to certain types of discovery packets. Only APs receiving responses from an AC can perceive that the AC is valid, and these APs can establish CAPWAP tunnels to the AC.

Notes

- If the AC discovery mode is set to supporting none of the discovery packets, an AP cannot connect to an AC using discovery packets.

Configuration Steps

Configuring AC Discovery via a Recommended Type of Discovery Packets

- Optional.

Command	**capwap discovery-type ac-referral { allow | forbidden}**
Parameter Description	**allow**: indicates that this type of discovery packets can be used to discover an AC. **forbidden**: indicates that this type of discovery packets cannot be used to discover an AC.
Defaults	An AP can send discovery packets of a recommended type to discover an AC by default.

Command Mode	AC configuration mode
Usage Guide	N/A

Configuring AC Discovery via Discovery Packets

- Optional.
- After this command is configured, configurations of other discovery types will be overwritten.

Command	**capwap discovery-type all { allow | forbidden}**
Parameter Description	**allow**: indicates that discovery packets can be used to discover an AC. **forbidden**: indicates that discovery packets cannot be used to discover an AC.
Defaults	An AP can send discovery packets to discover an AC by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring AC Discovery via DHCP Packets

- Optional.

Command	**capwap discovery-type dhcp { allow | forbidden}**
Parameter Description	**allow**: indicates that DHCP packets can be used to discover an AC. **forbidden**: indicates that DHCP packets cannot be used to discover an AC.
Defaults	An AP can send DHCP packets to obtain the AC address and discover the AC by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring AC Discovery via DNS Packets

- Optional.

Command	**capwap discovery-type dns { allow | forbidden}**
Parameter Description	**allow**: indicates that DNS packets can be used to discover an AC. **forbidden**: indicates that DNS packets cannot be used to discover an AC.
Defaults	An AP can send DNS packets to obtain the AC address and discover the AC by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring AC Discovery via Packets Carrying the Statically Configured AC IP Address

- Optional.

Command	**capwap discovery-type static-config { allow | forbidden}**

Parameter Description	**allow**: indicates that packets carrying the statically configured AC IP address can be used to discover an AC. **forbidden**: indicates that packets carrying the statically configured AC IP address cannot be used to discover an AC.
Defaults	An AP can send packets carrying the statically configured AC IP address to discover the AC by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring AC Discovery via Discovery Packets of Other Types

- Optional.
- Configure other AC discovery modes, such as the broadcast or multicast mode.

Command	**capwap discovery-type unknown { allow | forbidden}**
Parameter Description	**allow**: indicates that broadcast or multicast discovery packets can be used to discover an AC. **forbidden**: indicates that broadcast or multicast discovery packets cannot be used to discover an AC.
Defaults	An AP can send broadcast or multicast packets to discover an AC by default.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the configuration is successful.

Configuration Example

Forbidding an AP to Send Discovery Packets of a Recommended Type to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send discovery packets of a recommended type to discover the AC.
AC	`Ruijie(config)# ac-controller` `Ruijie(config-ac)# capwap discovery-type ac-referral forbidden`
Verification	● Display the AC configurations.
AC	`Ruijie#show running-config` `!` `ac-controller` `capwap discovery-type ac-referral forbidden` `!`

Forbidding an AP to Send Discovery Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send discovery packets to discover the AC.
AC	Ruijie(config)# ac-controller Ruijie(config-ac)# capwap discovery-type all forbidden
Verification	● Display the AC configurations.
AC	Ruijie#show running-config ! ac-controller capwap discovery-type all forbidden !

Forbidding an AP to Send DHCP Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send DHCP packets to obtain the AC address and discover the AC.
AC	Ruijie(config)# ac-controller Ruijie(config-ac)# capwap discovery-type dhcp forbidden
Verification	● Display the AC configurations.
AC	Ruijie#show running-config ! ac-controller capwap discovery-type dhcp forbidden !

Forbidding an AP to Send DNS Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send DNS packets to obtain the AC address and discover the AC.
AC	Ruijie(config)# ac-controller Ruijie(config-ac)# capwap discovery-type dns forbidden
Verification	● Display the AC configurations.
AC	Ruijie#show running-config ! ac-controller capwap discovery-type dns forbidden !

Forbidding an AP to Send Packets Carrying the Statically Configured AC IP Address to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send packets carrying the statically configured AC IP address to discover the AC.
AC	`Ruijie(config)# ac-controller` `Ruijie(config-ac)# capwap discovery-type static-config forbidden`
Verification	● Display the AC configurations.
AC	`Ruijie#show running-config` `!` `ac-controller` `capwap discovery-type static-config forbidden` `!`

↘ Forbidding an AP to Send Other Types of Discovery Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send other types of discovery packets to discover the AC.
AC	`Ruijie(config)# ac-controller` `Ruijie(config-ac)# capwap discovery-type unknown forbidden`
Verification	● Display the AC configurations.
AC	`Ruijie#show running-config` `!` `ac-controller` `capwap discovery-type unknown forbidden` `!`

Common Errors

N/A

3.5 Monitoring

Displaying

Description	Command
Displays the list of files activated on the AC.	**show ac-config active-file**
Displays the mapping between AP product series configured on the AC and product models, and files used to upgrade the product series.	**show ac-config serial-product**

Description	Command
Displays the information about the upgrade group configured on the AC.	show ac-config upgrade-group [*group-name*]
Displays the data on the master board of the AP.	**show ap-config board-data** *ap-name*
Displays the status of links between ACs and APs.	**show ap-config link-latency** { **all** | **single** *ap-name* }
Displays the AP vendor information.	**show ap-config inventory** *ap-name*
Displays the AP restart statistics	**show ap-config reboot** *ap-name*
Displays the mini AP information of a specified AP	**show ap-config slot**
Displays the static IP address of an AP	**show ap-config static-ip**{ **all** | **single** *ap-name* }
Displays the AP location information	**show ap-config summary location**
Displays the mini AP information of all APs	**show ap-configsummary slot**
Displays the AP upgrade status	**show ap-config updating-list**
Displays the AP status descriptions	**show ap-config wtp-descriptor** *ap-name*
Displays the AP status information	**show ap-config wtp-info** *ap-name*
Displays the detailed information about the CAPWAP tunnel	**show capwap** [index | [ip-address [port]]] **detail**
Displays the status of the CAPWAP tunnel	**show capwap state**
Displays the CAPWAP tunnel statistics	**show capwap** [index | [ip-address [port]]] **statistics**
Displays the AP version information	**show version** { **all** | *ap-name* }
Collects and displays various logs on an AP	**tran-data-start** *ap-name* {**exception** | **memory | tech-support** | **tech-package**} **tran-data-show** *ap-name* {**exception** | **cpuinfo** | **memory** | **syslog**| **tech-support**}
Displays all downlink ports of i-Share+ APs	**show ap-config summary slot interface**

4 Configuring WBS

4.1 Overview

The Wireless Basic Service (WBS) is used to configure wireless-specific parameters on access controllers (ACs) when thin access points (APs) are deployed.

Link integrity detection is a basic service of the WBS. It detects the wired uplinks on APs. When the links are disconnected, the access services of the APs are stopped to force users offline. When the links are restored, the APs continue to provide wireless access services. Enabling link integrity detection in a fit AP architecture with dense AP deployment helps reduce the network disconnection time and improve user experience.

Protocols and Standards

- 802.11n: Enhancements for Higher Throughput
- 802.11ac：Enhancements for Very High Throughput for Operation in Bands below 6 GHz
- 802.11ax：Enhancements for High Efficiency WLAN

4.2 Applications

Application	Description
Configuring Fit APs	Run commands on ACs to configure the parameters of fit APs.
Enabling Link Integrity Detection	Enable link integrity detection in a fit AP architecture to improve the quality of service (QoS) of wireless access.

4.2.1 Configuring Fit APs

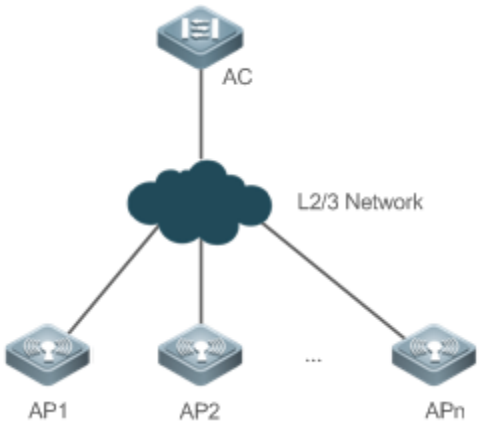
Scenario

Configure fit APs. Administrators can manage the configurations of fit APs on an AC in a centralized manner. Assume that a network has the following deployment requirements:

1. Allow the AC to monitor the status of the feeder links on i-Share APs.
2. Prevent stations (STAs) with received signal strength indication (RSSI) smaller than 20 from accessing the network.
3. Enable short guard interval (GI) in 20 MHz.
4. Prevent the use of low data rates, such as 1 Mbps, 2 Mbps, and 5.5 Mbps.

Figure 4-1 shows the fit AP networking topology.

Figure 4-1 Fit AP Networking Topology



Deployment

Main configuration points on the AC:

1. Enable i-Share antenna feeder link detection for all the APs and set the detection interval to an expected value.
2. Run **response-rssi** for the radios of all the APs and set the threshold to 20 dB.
3. Run **short-gi enable** for the radios of all the APs and set the bandwidth to 20 MHz.
4. Disable the use of the 1 Mbps, 2 Mbps, and 5.5 Mbps data rates for 802.11b/g network users.

4.2.2 Enabling Link Integrity Detection

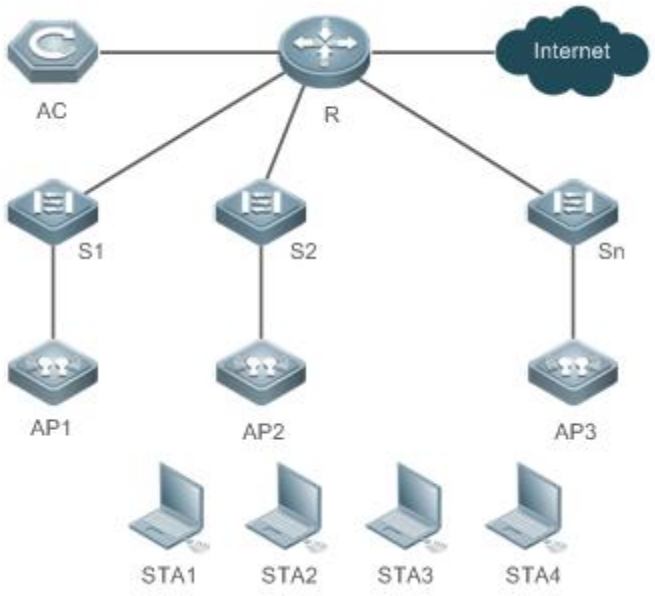
Scenario

Enable link integrity detection on wireless networks with a fit AP architecture.

See Figure 4-2.

- An AC is connected to the Internet through a router. AP1, AP2, and AP3 are connected to the router through three switches and associated with the AC.
- Station 1 (STA1) is associated with AP1, STA2 and STA3 are associated with AP2, and STA4 is associated with AP3. The STAs access the Internet through the AC.

Figure 4-2



Remarks	R is an egress router. S1, S2, and S3 are Layer-2 switches and function as the access devices for APs. AP1, AP2, and AP3 are directly connected to S1, S2, and S3.

Deployment

- Layer-2 switches provide the access service to APs.
- Router R sets up connections between ACs and APs and between STAs and the Internet.

4.3 Features

Basic Concepts

A-MPDU

The 802.11n standards adopt the aggregate MAC protocol data unit (A-MPDU). Multiple MPDUs are aggregated into an A-MPDU, and only one PHY header is retained whereas the PHY headers of other MPDUs are removed. In this way, the additional information of the PHY header of each MPDU to be transmitted is reduced, and the number of ACK frames is also reduced, which mitigates the burden and improves network throughput.

MCS

The physical layer of 802.11n supports high data transmission rates and is compatible with 802.11a/b/g rates. The many different speeds supported at the physical layer of 802.11n are called modulation and coding scheme (MCS) rates.

Beacon

The APs on wireless local area networks (WLANs) periodically send beacon frames externally. The beacon frames contain AP information. Wireless STAs receive beacon frames to discover WLANs.

RSSI

RSSI indicates the quality of wireless connections.

Country Code

A country code identifies a country with radio frequency (RF) usage. RFs, channels, and powers vary with different country codes. Before you configure an AP, determine the country code that the AP supports. If the configured country code is changed, the RFs, channels, and powers mapped to the country code are also changed.

Frequency Band

FR transmission in the 2.4 GHz and 5 GHz frequency bands is supported.

Channel

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. In China, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Transmit Power

Transmit power indicates the strength of the RF signals transmitted by an AP. It is proportional to the radio signal coverage area of the AP.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To avoid this problem, STAs are required to check the idle state of channels before sending data. If an STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer of the slot time (which is an operation time unit specified in the Media Access Control [MAC] protocol). The value of the backoff time is automatically subtracted by 1 each time after the slot time has elapsed. When the backoff time is reduced to 0, the STA starts sending data. The slot time on WLANs is classified into 20 μs and 9 μs, with the later being called short slot time.

Antenna Transmit/Receive Types

You can configure some antennas on an RF card to transmit signals and the other antennas to receive signals.

Short GI

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

Fragmentation Threshold

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports the fragmentation of packets before transmission. Packets are fragmented according to a threshold, which reduces the interference probability and saves bandwidth resources during retransmission.

RTS

To avoid channel conflicts and the resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called Request To Send/Clear To Send (RTS/CTS). When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. When multiple STAs send RTS frames to the same STA, only the STAs that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can resend RTS frames after a time because a channel conflict is considered to have occurred.

PHY Protection Modes

Frames can be transmitted in Greenfield mode or hybrid mode. The hybrid mode is intended to support compatibility with other physical layers, and the Greenfield mode is used to transmit physical layer headers at high speeds. A device which uses the high-throughput (HT) hybrid mode can transmit frames in 802.11a/b/g and 802.11n modes. Such a device first transmits a conventional format preamble, followed by an HT format preamble. The device must send a conventional CTS-to-Self or RTS/CTS frame before transmitting data. These protection mechanisms enable 802.11a/b/g devices, including those devices not connected to APs in HT hybrid mode to sense the busy state of channels.

Preamble Type

A preamble is a group of bits in a packet header, used to synchronize the transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to transmit than the data frames with a short preamble.

U-APSD

802.11e introduces Wi-Fi multimedia power save (WMM-PS) to reduce the delay of the services with high real-time requirements during the power management process. WMM-PS adopts the Unscheduled Automatic Power Save Delivery (U-APSD) technology to disable the transmission of radio signals during most of the time, which extends the battery life. U-APSD is an enhancement of the 802.11 power saving mechanism.

MU-MIMO

MU-MIMO is short for Multi-User Multiple-Input Multiple-Output. 802.11ac uses downlink MU-MIMO to enable an AP to send data to multiple STAs through beamforming. 802.11ax uses uplink MU-MIMO to enable multiple STAs to send data to an AP.

OFDMA

OFDMA is short for Orthogonal Frequency Division Multiple Access. OFDMA is a multi-user version of the popular orthogonal frequency-division multiplexing (OFDM) digital modulation scheme. Multiple access is achieved in OFDMA by assigning subsets of subcarriers to individual users. This allows simultaneous low-data-rate transmission from several users.

Overview

Feature	Description
Configuring i-Share Antenna Feeder Link Detection	Checks the status of the feeder links on i-Share APs.
Configuring STA Access Control	Controls the access of specified wireless STAs.
Configuring AP RF Parameters	Configures the RF parameters for APs or radios.
Configuring Data Rate Control Parameters	Configures the RF parameters of data rate control.
Configuring Power-Save Parameters	Sets the parameters of power saving.
Enabling Link Integrity Detection	Detects the integrity of links to improve the wireless service quality.
Configuring E-Bag Parameters	Provides a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.
Configuring WLANs in One-Click Mode	Provides the one-click WLAN configuration feature to perform fast configuration on devices with zero configurations.

4.3.1 Configuring STA Access Control

Working Principle

Ruijie Networks provides wireless STA access control.

Wireless STAs search for APs through active scan and passive scan.

- Active scan: A wireless STA sends a Probe Request frame to request access to an AP, which will respond with a Probe Response frame.
- Passive scan: APs broadcast beacon frames periodically. Wireless STAs listen to beacon frames and initiate connections to APs.

To control the network coverage areas of APs and improve the transmission quality of radio signals, the following methods are used to limit the access of wireless STAs:

- Control the beacon frame broadcast ranges of APs to limit the access of long-distance wireless STAs.
- Control the minimum RSSI value applied to wireless STAs during the access process. The STAs which send request frames with RSSI smaller than the minimum value are denied access.
- Control the minimum RSSI value applied to wireless STAs during the data transmission process. The STAs which send data frames with RSSI smaller than the minimum value are forced offline. Then the STAs can roam to other APs with better radio signals.

4.3.2 Configuring AP RF Parameters

You can configure the RF parameters for APs and radios.

Working Principle

A-MPDU

The 802.11n standards adopt A-MPDU. Multiple MPDUs are aggregated into an A-MPDU, and only one PHY header is retained whereas the PHY headers of other MPDUs are removed. In this way, the additional information of the PHY header of each MPDU to be transmitted is reduced, and the number of ACK frames is also reduced, which mitigates the burden and improves network throughput.

MCS

In 802.11n, RF rates are configured by using the index values of the MCS, which is used to express the communication rates on WLANs. The MCS is a rate table. The table columns show the factors of concern that affect communication rates, and the table rows show the MCS indexes. Each MCS index maps a physical transmission rate which is determined by a group of parameters. For the description of all the MCS rate tables, see the *IEEE P802.11n D2.00*.

Wireless Channel

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries and frequency bands. In China, the 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13), and the 5 GHz frequency band can be configured with five channels (channels 149, 153, 157, 161, and 165). The overlapping channels in the 2.4 GHz frequency band generate interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision. The five channels in the 5 GHz frequency band do not overlap or generate interference.

Packet Fragmentation

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports the fragmentation of packets before transmission. Packets are fragmented according to a threshold, which reduces the interference probability and saves bandwidth resources during retransmission.

RTS/CTS

To avoid channel conflicts and the resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called RTS/CTS. When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. When multiple STAs send RTS frames to the same STA, only the STAs that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can resend RTS frames after a time because a channel conflict is considered to have occurred.

If each STA implements RTS/CTS handshake before sending data, many RTS frames will occupy channel bandwidths. To avoid this problem, you can configure an RTS threshold to specify the frame length of transmitted data. If an STA sends data with a frame length smaller than the RTS threshold, the STA will not implement RTS/CTS handshake.

Beacon

The APs on WLANs periodically send beacon frames externally. The beacon frames contain AP information. Wireless STAs receive beacon frames to discover WLANs.

Preamble Type

A preamble is a group of bits in a packet header, used to synchronize the transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to transmit than the data frames with a short preamble.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To avoid this problem, STAs are required to check the idle state of channels before sending data. If an STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer of the slot time (which is an operation time unit specified in the MAC protocol). Assume that the random integer is 3. The value of the backoff time is automatically subtracted by 1 each time after the slot time has elapsed. When the backoff time is reduced to 0, the STA starts sending data. Reducing the slot time can reduce the overall backoff time and increase network throughput.

Channel Bandwidth

In 802.11n, two 20 MHz bandwidths are combined into a 40 MHz bandwidth, which can be used as two 20 MHz bandwidths. (One 20 MHz bandwidth is the primary bandwidth, and the other is the secondary bandwidth. Data can be received and transmitted by using the 40 MHz bandwidth or two individual 20 MHz bandwidths.) In this way, data rates are doubled and wireless network throughput is increased.

GI

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

802.11ax supports three types of guard interval: 0.8us, 1.6us, and 3.2us.

Country Code

A country code identifies a country with RF usage. RFs, channels, and powers vary with different country codes. Before you configure an AP, determine the country code that the AP supports. If the configured country code is changed, the RFs, channels, and powers mapped to the country code are also changed.

Antenna Transmit/Receive Types

APs use different quantities of antennas for transmitting and receiving signals, which enables APs to use two or three spatial streams to transmit signals in 802.11n mode, thus improving data transmission performance.

Internal Antenna and External Antenna

Internal antennas are integrated inside the enclosures of APs, and external antennas are connected to the reserved hardware interfaces of APs. External antennas achieve longer transmission distances than internal antennas with the same transmission power.

Omnidirectional Antenna and Directional Antenna

- An omnidirectional antenna radiates equally in all directions. A directional antenna radiates in a specific direction with a cone-shaped radiation range.**Maximum Distance of Radio Transmission Between AP Radios and the Peer End**

Radio signals are transmitted in space at the speed of light. The longer the distance of radio transmission between AP radios and the peer end, the longer time it takes to transmit radio packets in space and the longer the timeout time for APs to wait for ACK and CTS frames. The timeout time must be adjusted based on the distance of radio transmission between AP radios and the peer end; otherwise, radio data transmission will fail. A very long timeout time will cause resource waste on the air interface when APs are still waiting for ACK and CTS frames. Configuring Data Rate Control Parameters

You can configure the RF parameters of data rate control.

Working Principle

802.11 is the industry standards that the Institute of Electrical and Electronics Engineers (IEEE) developed for WLAN communications. 802.11x is an improvement over 802.11. The main transmission standards include 802.11b, 802.11a, 802.11g, and 802.11n.

1. 802.11b

The operating band is 2.4 GHz, and the data transmission rate can reach 11 Mbps, which can be reduced to 5.5 Mbps, 2 Mbps, or 1 Mbps based on actual requirements.

2. 802.11a

The operating band is 5 GHz, and the data transmission rate can reach 54 Mbps, which can be reduced to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps based on actual requirements.

3. 802.11g

The operating band is 2.4 GHz, and the data transmission rate can reach 54 Mbps, which can be reduced to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps based on actual requirements. 802.11g STAs are backward compatible with 802.11b.

4.3.3 Configuring Power-Save Parameters

Working Principle

↘ DTIM Period

A delivery traffic indication map (DTIM) is a flag bit in a beacon frame, used to determine the interval at which an AP sends broadcast or multicast frames. APs buffer the data that wireless STAs in dormant state need to receive according to the DTIM period. After the DTIM period has elapsed, APs send the buffered data to wireless STAs.

The DTIM period is expressed based on the number of sent beacon frames. Assume that the DTIM period is set to 3. APs send broadcast or multicast frames each time after three beacon frames are sent.

↘ U-APSD Power Saving

U-APSD is an improvement over the power saving mode. When clients are associated with ACs, the clients can configure which ACs have the trigger attribute, which ACs have the delivery attribute, and the maximum number of packets to be sent after trigger. The trigger and delivery attributes can be modified when flows are created through connection access control (CAC). When a client sleeps, the delivery-enabled AC packets destined for the client are buffered. To retrieve the buffered packets, the client needs to send trigger-enabled AC packets. After receiving the trigger-enabled AC packets, the AP sends

the buffered packets according to the to-be-sent packet quantity determined during the access process. Other AC packets than delivery-enabled AC packets are stored and transmitted in accordance with the 802.11 standards.

4.3.4 Enabling Link Integrity Detection

APs are wireless access devices without the switching feature. They implement all functions of the physical layer and partial functions of the MAC layer. A fat AP or fit AP has only one wired uplink, which is the data channel allowing STAs to access the AP. When the wired uplink is disconnected because of a fault, all the wireless STAs connected to the AP cannot access the Internet.

Wireless STAs cannot sense link disconnections immediately or take measures; as a result, the network connection cannot be restored for a long time.

Link integrity detection is designed to solve this problem.

Working Principle

The link integrity detection function continuously detects the status of the wired uplinks on APs. When a wired uplink is disconnected, the RF interface of the AP is disabled to stop the access service. The wireless STAs associated with the AP are forced offline and have to reconnect to other normal APs.

When the wired uplink is recovered, the link integrity detection function enables the RF interface of the AP again to restore the wireless access service.

Link integrity detection enables the wireless STAs that are associated with APs with disconnected wired uplinks to reconnect to other normal APs.

4.3.5 Configuring E-Bag Parameters

You can configure the E-bag parameters for APs and radios.

Working Principle

You can run a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.

↘ A-MPDU

A-MPDU is short for aggregate MAC protocol data unit.

↘ LDPC

A low-density parity-check (LDPC) code is a linear error correcting code. Being easy to use and with low complexity, this coding method adopts the forward error correction (FEC) technology to improve the coding reliability and gains. LDPC was developed at the beginning of the 1960 and supports the transmission of information in noisy frequencies with massive background or content damage. It also greatly reduces the probability of information loss during transmission in frequencies with serious noise interference. However, a small number of STAs are not compatible with LDPC, and enabling LDPC will result in packet loss.

↘ STBC

Space time block coding (STBC) is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas at different time points to improve the reliability of data transmission by means of time diversity and space diversity. The outstanding advantage of STBC is the use of maximum likelihood decoding to obtain complete antenna gains. Some STAs may not be compatible with STBC.

A-MPDU Software Retransmission Times

The A-MPDU software retransmission mechanism is designed to avoid the loss of sub-frames in wireless communications. The greater the retransmission times, the lower the probability of sub-frame loss. If packets are retransmitted frequently, the burden on the air interface is increased, which affects the real-time transmission of packets on the air interface. You can increase the retransmission times if you need to avoid packet loss when there is a high probability of sub-frame loss.

A-MPDU-RTS

The RTS protection feature of A-MPDU prevents resource waste on the air interface caused by packet collision due to hidden nodes. Because RTS interaction consumes air interface resources and has resulting adverse impact in many application scenarios, this feature is disabled by default. Enable RTS protection only when the resource waste on the air interface caused by hidden nodes is greater than the resource consumption of RTS interaction on the air interface.

Single-Time Received Ethernet Packet Quantity

A command is provided to adjust the number of Ethernet packets received at a single time. Increasing Ethernet packet reception can improve network performance but may reduce APs' ability to handle key packets in real time. You can reduce Ethernet packet reception when the requirements for performance are not high but user concurrency and real-time packet handling are demanded. In this case, it is recommended that the single-time received Ethernet packet quantity be set to 25.

4.3.6 Configuring WLANs in One-Click Mode

The one-click WLAN configuration feature allows you to perform fast configuration on devices with zero configurations.

Working Principle

autowifi

Perform the following configuration on an AC:

1. Division of virtual local area networks (VLANs): On the AC, configure VLAN1 as the VLAN for APs and VLAN2 as the VLAN for STAs.
2. Address pool: On the AC, configure the 192.168.1.0 network segment as the address pool for APs and configure the 192.168.2.0 network segment as the network segment for STAs. The default IP addresses of VLAN1 and VLAN2 are 192.168.1.1 and 192.168.2.1 respectively. The default management IP address is 88.88.88.88.
3. WLAN configuration: Name the WLAN **autowifi**_*XXXX*. The last four characters are the last four digits of the MAC address of the AC. You can use wlan-id 1.
4. Security: By default, WPA2 encryption is used. The password is **autowifi**.
5. WLAN-VLAN mapping: On the AC, configure the mapping between wlan-id 1 and VLAN2 in the group named **ap-group default**.

6. Service: Enable the Dynamic Host Configuration Protocol (DHCP) service.

4.3.7 Managing the Operating Frequency Band When Power Supply Is Insufficient

For an AP that requires the PoE+ mode but the power supply device negotiates not the PoE+ mode but the 15.4 W power, power supply may be insufficient if all RF modules provide services. When power supply is insufficient, the AP disables some RF modules (2.4 GHz or 5 GHz) based on its capabilities and external power supply conditions to ensure that other RF modules have sufficient power and can run properly. When the power supply mode is changed to PoE+, all RF modules are enabled and can run properly.

Working Principle

For an AP that requires the PoE+ mode but the negotiated power upon startup is 15.4 W, the AP disables some RF modules (2.4 GHz or 5 GHz) based on its capabilities. However, the AC can switch the operating frequency band of the AP, that is, switching between 2.4 GHz and 5 GHz.

4.4 Configuration

Configuration	Description and Command	
Configuring STA Access Control	(Optional) It is used to configure STA access control.	
	{**802.11a** | **802.11b**} **network** {**enable** | **disable**}	Enables or disables the 2.4 GHz or 5 GHz network.
	11asupport enable	Enables 802.11a support for specified AP radios in 5 GHz.
	11bsupport enable	Enables 802.11b support for specified AP radios in 2.4 GHz.
	11gsupport enable	Enables 802.11g support for specified AP radios on the 2.4 GHz network.
	11nasupport enable	Enables 802.11n support for specified AP radios in 5 GHz.
	11ngsupport enable	Enables 802.11n support for specified AP radios in 2.4 GHz.
	11acsupport enable	Enables 802.11ac support for specified AP radios.
	11axsupport enable	Enables 802.11ax support for specified AP radios.
	coverage-area-control	Configures the management frame power for APs.
	extra-coverage	Configures the third radio for user access.
	response-rssi	Configures the minimum RSSI for wireless STAs to connect to specified AP radios.

Configuration	Description and Command	
	assoc-rssi	Configures the minimum RSSI for wireless STAs to maintain connections to specified AP radios.
Configuring AP RF Parameters	(Optional) It is used to configure the RF parameters for APs.	
	802.11n a-mpdu enable	Enables A-MPDU for specified AP radios.
	802.11n mcs support	Configures the maximum 802.11n MCS index value for specified AP radios.
	802.11ac mcs support	Configures the maximum 802.11ac MCS index value for specified AP radios.
	802.11ax mcs support	Configures the maximum 802.11ax MCS index value for specified AP radios.
	antenna	Configures the antenna transmit/receive type for specified AP radios.
	external-antenna enable	Enables usage of external antennas for specified AP radios, and disables usage of internal antennas.
	antenna type	Configures an omnidirectional antenna or a directional antenna.
	beacon dtim-period	Configures the DTIM period for specified AP radios.
	beacon period	Configures the beacon frame transmission period for specified AP radios.
	chan-with	Configures bandwidth assignments for specified AP radios.
	channel	Configures channel assignments for specified AP radios.
	channel-switch	Configures channel switching.
	country	Configures the country code set supported by an AC or the country code used by AP radios.
	enable-radio	Enables specified or all AP radios.
	fragment-threshold	Configures the fragmentation threshold for specified AP radios.
	green-field enable	Enables the protection mode for specified AP radios.
	ofdma	Enables ofdma for the specified radio.
	power local	Configures the transmit power for specified AP radios.

Configuration	Description and Command	
	radio-optimize	Configures radio parameters, including power, channel and antenna type.
	radio-type	Specifies the operating band for specified AP radios.
	rts-threshold	Configures the RTS threshold for specified AP radios.
	short-gi	Enables short GI for specified AP radios.
	update-key-tsc enable	Enables TKIP Sequence Counter (TSC) update for APs during 802.11x re-authentication.
	peer-distance	Configures the maximum distance of wireless transmission between APs and the peer end.
	mu-mimo enable	Configures MIMO for multi users.
	mcell	Configures mcell.
Configuring Data Rate Control Parameters	(Optional) It is used to configure the parameters of data rate control.	
	802.11a network rate	Configures the data rate set supported by 802.11a STAs.
	802.11b network rate	Configures the data rate set supported by 802.11b STAs.
	802.11g network rate	Configures the data rate set supported by 802.11g STAs.
	mcast-rate	Configures the WLAN multicast rate.
	beacon rate	Configures the beacon frame transmission rate.
Configuring Power-Save Parameters	(Optional) It is used to configure the power-save parameters.	
	beacon dtim-period	Configures the DTIM period.
	apsd	Enables or disables U-APSD power saving.
Enabling Link Integrity Detection	(Mandatory) It is used to enable link integrity detection.	
	link-check enable	Enables link integrity detection.
Configuring E-Bag Parameters	(Optional) It is used to configure the parameters of E-bag.	
	ampdu-retries	Configures the A-MPDU software retransmission times.
	ampdu-rts	Enables or disables RTS protection for A-MPDU packets.

Configuration	Description and Command	
	eth-schd	Configures the single-time received Ethernet packet quantity for APs.
	ldpc	Enables or disables LDPC.
	stbc	Enables or disables transmit/receive STBC.
	ebag	Configures E-bag network optimization in one-click mode.
Configuring WLANs in One-Click Mode	⚠ (Optional) It is used to configure WLANs in one-click mode.	
	autowifi	Configures WLANs in one-click mode.
Managing the Operating Frequency Band When Power Supply Is Insufficient	**hap-poe enable radio** { **802.11a** | **802.11b** }	Switches to 2.4 GHz or 5 GHz.

4.4.1 Configuring STA Access Control

Configuration Effect

- Control the access of a specified type of wireless STAs to manage these wireless STAs conveniently.

Configuration Steps

↘ Enabling or Disabling the 2.4 GHz or 5 GHz Network

- Optional.
- Enable or disable the 2.4 GHz or 5 GHz network on an AC.
- The AC assigns the network settings to all the APs to instruct the APs to enable or disable the 2.4 GHz or 5 GHz network.

Command	{ **802.11a** | **802.11b**} **network** { **enable** | **disable** }
Parameter Description	N/A
Defaults	By default, the 2.4 GHz and 5 GHz networks are enabled.
Command Mode	AC configuration mode
Configuration Usage Guide	N/A

↘ Enabling 802.11a Support

- Optional.
- The configuration takes effect only when the AP radios operate in 5 GHz.
- On the AC, enable 802.11a support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11a STAs in 5 GHz.

Command	**11asupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11a support. The value ranges from 1 to 96.
Defaults	By default, the access of 802.11a STAs is supported in 5 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 5 GHz. The configuration is supported only by certain APs.

Enabling 802.11b Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11b support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11b STAs in 2.4 GHz.

Command	**11bsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11b support. The value ranges from 1 to 96.
Defaults	By default, the access of 802.11b STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11g Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11g support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11g STAs in 2.4 GHz.

Command	**11gsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11g support. The value ranges from 1 to 96.
Defaults	By default, the access of 802.11g STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode

Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11na Support

- Optional.
- The configuration takes effect only when the AP radios operate in 5 GHz.
- On the AC, enable 802.11na support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11n STAs in 5 GHz.

Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11na support. The value ranges from 1 to 96.
Defaults	By default, the access of 802.11n STAs is supported in 5 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 5 GHz. The configuration is supported only by certain APs.

Enabling 802.11ng Support

- Optional.
- The configuration takes effect only when the AP radios operate in 2.4 GHz.
- On the AC, enable 802.11ng support for specified APs.
- The AC assigns the settings to the APs to instruct the APs to support the access of 802.11n STAs in 2.4 GHz.

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11ng support. The value ranges from 1 to 96.
Defaults	By default, the access of 802.11n STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz. The configuration is supported only by certain APs.

Enabling 802.11ac

- Optional.
- On the AC, enable 802.11ac support for specified APs.
- The AC delivers configuration to the APs to instruct the APs to support the access of 802.11ac STAs.

Command	**11acsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11ac support. The value ranges from 1 to 96.
Defaults	Only the radios with even IDs support the access of 802.11ac STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling 802.11ax

- Optional.
- On the AC, enable 802.11ax support for specified APs.
- The AC delivers configuration to the APs to instruct the APs to support the access of 802.11ax STAs.

Command	**11axsupport enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with 802.11ax support. The value ranges from 1 to 96.
Defaults	Only the radios with even IDs support the access of 802.11ax STAs.
Command Mode	AP configuration mode, all-AP configuration mode
Configuration Usage Guide	N/A

Configuring the Management Frame Power for APs

- Optional.
- Perform the configuration only on the required device unless otherwise specified.
- On the AC, configure the management frame power for specified APs.
- The AC assigns the settings to the APs to instruct the APs to use the configured management frame transmit power. In this way, the signal coverage areas of the APs are controlled to limit the access of wireless STAs.

Command	**coverage-area-control** *power* [**radio** { *radio-id* | **802.11b | 802.11a** }]
Parameter Description	*power*: specifies the management frame power. The value ranges from 0 to 32, in the unit of dBm. *radio-id*: specifies the IDs of the radios assigned with channels. The value ranges from 1 to 96. **802.11b**: indicates that bandwidth is assigned to all the radios in 2.4 GHz. **802.11a**: indicates that bandwidth is assigned to all the radios in 5.8 GHz.
Defaults	By default, the management frame power for APs is 0 dBm.
Command Mode	AP configuration mode/AP group configuration mode

Configuration Usage Guide	N/A

Configuring the Minimum RSSI for Wireless STAs to Access APs

- Optional.
- On the AC, configure the minimum RSSI for wireless STAs to access specified AP.
- The AC assigns the settings to the APs to instruct the APs to use the configured minimum RSSI as the threshold for allowing the access of wireless STAs.

Command	**response-rssi** *rssi* **radio** {*radio-id* | *[802.11b* | *802.11a*]}
Parameter Description	*rssi:* specifies the minimum RSSI for wireless STAs to access APs. The value ranges from 0 to 100, in the unit of dB. *radio-id*: specifies the IDs of the radios assigned with the minimum RSSI. The value ranges from 1 to 96. *802.11b*: indicates that the minimum RSSI is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the minimum RSSI is assigned to all the radios in 5.8 GHz.
Defaults	By default, the RSSI is set to **0**, indicating that there is no RSSI limit on the access of wireless STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, the minimum RSSI is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

Configuring the Minimum RSSI for Wireless STAs to Maintain Connections to APs

- Optional.
- On the AC, configure the minimum RSSI for wireless STAs to maintain connections to specified AP.
- The AC assigns the settings to the APs to instruct the APs to use the configured minimum RSSI as the threshold for maintaining the connections of wireless STAs.

Command	**assoc-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi:* specifies the minimum RSSI for wireless STAs to maintain connections. The value ranges from 0 to 100, in the unit of dB. *radio-id*: specifies the IDs of the radios assigned with the minimum RSSI. The value ranges from 1 to 96.
Defaults	By default, the RSSI is set to **0**, indicating that there is no RSSI limit on the access of wireless STAs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring the Third Radio for User Access

- Optional.
- On the AC, configure the AP in high density scenario.
- The channel, antenna, power, bandwidth will be adjusted for better access experience.

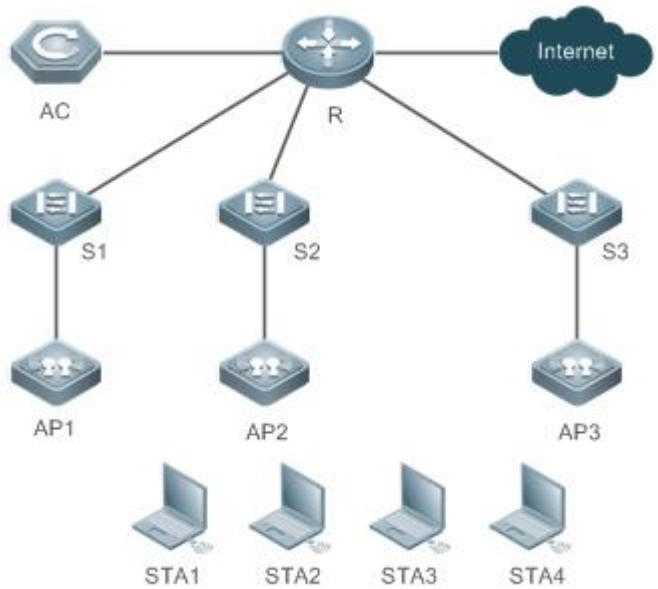
Command	**extra-coverage enable**
Parameter Description	N/A
Defaults	The third radio is disabled by default.
Command Mode	AP configuration mode AP group configuration mode
Configuration Usage Guide	Use the **no** form of this command to disable the function. Use teh **default** form of this command to restore the default setting,

Verification

- Run **show ap-config running** *ap-name* to display the parameter settings of STA access control.

Configuration Example

↘ Configuring the Parameters of STA Access Control

Scenario **Figure 4-3**	 In Figure 4-3, an AC is connected to fit APs. On the AC, configure STA access control for all the APs according to the following step: 1. Disable the 2.4 GHz network.

	On the AC, configure STA access control for AP1 according to the following steps: 1. Enable the access of 802.11a and 802.11na STAs in 5 GHz 2. Enable the access of 802.11g and 802.11ng STAs in 2.4 GHz. 3. Enable the access of 802.11ac STAs. 4. Set the management frame power to 20 dBm. 5. Set the minimum RSSI for wireless STAs to access APs to 20 dB. 6. Set the minimum RSSI for wireless STAs to maintain connections to15 dB. 7. Enable the third radio for user access.
Configuration Steps	● Disable the 2.4 GHz network on the AC.
AC	Ruijie# configure terminal Ruijie(config)# ac-controller Ruijie(config-ac)# 802.11b network disable
	● Set the STA access control parameters for AP1 on the AC.
AC	Ruijie# configure terminal Ruijie(config)# ap-config AP1 Ruijie(config-ap)# 11asupport enable radio 2 Ruijie(config-ap)# 11nasupport enable radio 2 Ruijie(config-ap)# 11gsupport enable radio 1 Ruijie(config-ap)# 11ngsupport enable radio 1 Ruijie(config-ap)# 11acsupport enable radio 1 Ruijie(config-ap)# no 11bsupport enable radio 1 Ruijie(config-ap)# coverage-area-control 20 Ruijie(config-ap)# response-rssi 20 radio 1 Ruijie(config-ap)# response-rssi 20 radio 2 Ruijie(config-ap)# assoc-rssi 15 radio 1 Ruijie(config-ap)# assoc-rssi 15 radio 2
Verification	● Run **show running** to check whether the 2.4 GHz or 5 GHz network is enabled or disabled.
AC	Ruijie(config)# show running !

	ac-controller sta-limit 1024 no capwap dtls enable 802.11b network disable country CN country US !
	● Run **show ap-config running** *ap-name* to display the STA access control parameters for AP1.
AC	Ruijie(config)# show ap-config running AP1 ! ap-config 220em no 11bsupport enable radio 1 coverage-area-control 20 response-rssi 20 radio 1 response-rssi 20 radio 2 assoc-rssi 15 radio 1 assoc-rssi 15 radio 2 radio-type 1 802.11b radio-type 2 802.11a !

4.4.2 Configuring AP RF Parameters

Configuration Effect

- Configure the RF parameters for APs and radios for easier configuration management.

Configuration Steps

↘ Enabling A-MPDU

- Optional.
- On an AC, enable A-MPDU for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to enable A-MPDU.

Command	**802.11n a-mpdu enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with A-MPDU. The value ranges from 1 to 96.

Defaults	By default, A-MPDU is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode. The configuration is supported only by certain APs.

Configuring the Maximum 802.11n MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11n MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11n MCS index value.

Command	**802.11n mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: specifies the MCS index value, which ranges from 0 to 23. *radio-id*: specifies the IDs of the radios assigned with the maximum 802.11n MCS index value. The value ranges from 1 to 96.
Defaults	By default, the maximum 802.11n MCS index value is 23.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring the Maximum 802.11ac MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11ac MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11ac MCS index value.

Command	**802.11ac mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: specifies the MCS index value, which ranges from 0 to 96. *radio-id*: specifies the IDs of the radios assigned with the maximum 802.11ac MCS index value. The value ranges from 1 to 48.
Defaults	By default, the maximum 802.11n MCS index value is 29.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11ac mode.

Configuring the Maximum 802.11ax MCS Index Value

- Optional.

- On an AC, configure the maximum 802.11ax MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11ax MCS index value.

Command	**802.11ax mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: specifies the MCS index value, which ranges from 0 to 95. *radio-id*: specifies the IDs of the radios assigned with the maximum 802.11ac MCS index value. The value ranges from 1 to 96.
Defaults	By default, the maximum 802.11n MCS index value is 95.
Command Mode	AP configuration mode
Configuration Usage Guide	1. The configuration takes effect only when the AP radios operate in 802.11ax mode. 2. Number of spatial streams = Maximum MCS index value/12 +1. For example, if the maximum MCS index value is 31, the maximum number of spatial streams is 3.

Configuring the Antenna Transmit/Receive Type

- Optional.
- On an AC, configure the antenna transmit/receive type for specified APs. Then the AC assigns the settings to the APs to instruct the APs to use the specified antenna selection masks to send and receive packets.

Command	**antenna** { **transmit** | **receive** } *value* **radio** *radio-id*
Parameter Description	**transmit**: is the antenna transmit parameter. **receive**: is the antenna receive parameter. *value*: specifies the antenna selection mask. The value ranges from 1 to 7. *radio-id*: specifies the IDs of the radios assigned with the antenna transmit/receive type. The value ranges from 1 to 96.
Defaults	In AP configuration mode, the default antenna selection mask varies with different product models and antenna quantities and is determined based on the product model. By default, no antenna transmit/receive type is configured in AP group configuration mode.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring Usage of External Antennas for APs

- Optional.
- On an AC, configure usage of external antennas for specified APs. Then the AC assigns the settings to the APs to instruct the APs to enable external antennas and disable internal antennas.

Command	**external-antenna enable radio** *radio-id*

Parameter Description	*radio-id*: specifies the IDs of the radios enabled with external antenna usage. The value ranges from 1 to 96.
Defaults	By default, usage of internal antennas is enabled, and usage external antennas is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring Omnidirectional Antennas or Directional Antennas

- Optional.
- After this command is configured, the AC delivers the configuration to an AP to notify the AP of the antenna to be used.

Command	**antenna type { omnidirection | direction } [radio** *radio-id*]
Parameter Description	**omnidirection**: Specifies an omnidirectional antenna. **direction**: Specifies a directional antenna. *radio-id*: Specifies the ID of a radio. The value ranges from **1** to **96**.
Defaults	An omnidirectional antenna is used by default.
Command Mode	AP configuration mode, all-AP configuration mode, and AP group configuration mode
Usage Guide	1. This configuration is valid only to radios supporting both omnidirectional antennas and directional antennas. 2. If the internal antennas and external antennas can be switched, the configuration of internal and external antennas takes effect prior to that of omnidirectional and directional antennas. 3. When no radio is specified, the configuration takes effect on all radios of an AP. 4. The **antenna type omnidirection** and **antenna type direction radio** *radio-id* commands cannot be simultaneously configured for a specific AP/AP group/all APs; otherwise, the later configuration overwrites the previous configuration.

Configuring the Beacon Frame Transmission Period

- Optional.
- On an AC, configure the beacon frame transmission period for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit beacon frames according to the configured period.

Command	**beacon period** *milliseconds* **radio** *radio-id*
Parameter Description	*milliseconds*: specifies the beacon frame transmission period. The value ranges from 20 to 1000, in the unit of ms. *radio-id*: specifies the IDs of the radios assigned with the beacon frame transmission period. The value ranges from 1 to 96.
Defaults	By default, the beacon frame transmission period is 100 ms.

Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring Bandwidth Assignments

- Optional.
- On an AC, configure bandwidth assignments for specified APs. Then the AC assigns the settings to the APs to instruct the APs to switch the channel bandwidth to the specified bandwidth.

Command	**chan-width** { **20** | **40 | 80 | 160** } **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	**20**: specifies the 20 MHz bandwidth. **40**: specifies the 40 MHz bandwidth. **80**: specifies the 80 MHz bandwidth. **160**: Specifies the **160** MHz bandwidth. *radio-id*: specifies the IDs of the radios assigned with bandwidth. The value ranges from 1 to 96. **802.11b**: indicates that bandwidth is assigned to all the radios in 2.4 GHz. **802.11a**: indicates that bandwidth is assigned to all the radios in 5.8 GHz.
Defaults	The default channel bandwidth of 5.8G radio on 802.11ax new products is 40 Mbps. The default channel bandwidth of the other radio is 20 Mbps.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, the bandwidth is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The bandwidth configuration takes effect only when APs operate in 802.11n or 802.11ac mode.

Configuring Channel Assignments

- Optional.
- On an AC, configure channel assignments for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to operate in specified channels.

Command	**channel** *channel-id* **radio** *radio-id* | **802.11b | 802.11a** }
Parameter Description	*channel-id*: specifies the operating channels of AP radios. *radio-id*: specifies the IDs of the radios assigned with channels. The value ranges from 1 to 96. **802.11b**: indicates that bandwidth is assigned to all the radios in 2.4 GHz. **802.11a**: indicates that bandwidth is assigned to all the radios in 5.8 GHz.
Defaults	The radio resource management (RRM) system automatically adjusts channels. By default, no channel assignments are configured.
Command Mode	AP configuration mode

Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring the Country Code Set Supported by an AC

- Optional.
- Add a country code to the country code set supported by an AC before you configure AP radios to use the country code.

Command	**country** *country-code*
Parameter Description	*country-code*: specifies the country code to be added.
Defaults	The country code set supported by the AC is {"CN"}.
Command Mode	AC configuration mode
Configuration Usage Guide	The country code "CN" supported by the AC cannot be deleted.

Configuring a Country Code

- Optional.
- Ensure that the configured country code is in the country code set supported by an AC. The AC will assign the settings to the APs to instruct the APs to use the configured country code.

Command	**country** *country-code* **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*country-code*: specifies the country code to be added. *radio-id*: specifies the IDs of the radios assigned with the country code. The value ranges from 1 to 48. *802.11b*: indicates that the country code is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the country code is assigned to all the radios in 5.8 GHz.
Defaults	The country code used by APs is "CN".
Command Mode	AP configuration mode
Configuration Usage Guide	1. The country code "CN" supported by the AC cannot be deleted. 2. The configuration is supported only by certain APs. 3. Before you configure APs, determine the country code set supported by the AC. If the country code used by an AP is changed, the RF band, channel, and power for the AP are also changed. 4. If you select **802.11b**, the country code is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. 5. 2.4 GHz radios do not support channel 14.

Configuring the Country Code Set Supported by an AC

- Optional.
- Add a country code to the country code set supported by an AC before you configure AP radios to use the country code.

Command	**country-code** *country-code*
Parameter Description	*country-code*: specifies the country code to be added.
Defaults	The country code set supported by the AC is CN.
Command Mode	AP configuration mode
Configuration Usage Guide	The country code "CN" supported by the AC cannot be deleted. The following country codes are available for choice:

Code	Country
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolvia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia

EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy
JO	Jordan
JP	Japan
KP	North Korea
KR	Korea ROC
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Macedonia
MO	Macau
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria

NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovak Republic
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad & Tobago
TW	Taiwan
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

Enabling Radios

- Optional.
- Enable radios on an AC. Then the AC assigns the settings to the APs to instruct the APs to enable the corresponding radios.

Command	**enable-radio** { *radio-id* | **all** }
Parameter Description	*radio-id*: specifies the IDs of the radios to be enabled. The value ranges from 1 to 96. **all**: indicates that all radios are enabled.
Defaults	By default, radios are enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	When radios are enabled or disabled, the wireless STAs connected to the radios will go offline. The configuration is supported only by certain APs.

Configuring the Fragmentation Threshold

- Optional.
- On an AC, configure the fragmentation threshold for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to perform fragment logic processing according to the configured threshold.

Command	**fragment-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: specifies the fragmentation threshold, which must be an even number ranging from 256 to 2346. *radio-id*: specifies the IDs of the radios assigned with the fragmentation threshold. The value ranges from 1 to 96.
Defaults	The default fragmentation threshold is 2346 bytes.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Enabling the Protection Mode

- Optional.
- On an AC, enable the protection mode for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to enable the protection mode.

Command	**green-field enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with the protection mode. The value ranges from 1 to 96.
Defaults	By default, the protection mode is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 2.4 GHz.

Configuring the Transmit Power

- Optional.
- On an AC, configure the transmit power for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the transmit power.

Command	**power local** *power***radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*power*: specifies the percent of transmit power for APs. The value ranges from 1 to 100. *radio-id*: specifies the IDs of the radios assigned with the transmit power. The value ranges from 1 to 96. *802.11b*: indicates that the transmit power is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the transmit power is assigned to all the radios in 5.8 GHz.
Defaults	The RRM system automatically adjusts the transmit power. By default, no transmit power is configured.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	If you select **802.11b**, the transmit power is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The configuration is supported only by certain APs.

Configuring a Frequency Band

- Optional.
- After a frequency band is assigned to AP radios, the RRM module analyzes the operating channel of the AP radios in global mode, adjusts the channel, and assigns the optimal channel to the AP. The AP radios are instructed to operate in the specified channel.

Command	**radio-type** *radio-id* { **802.11a** | **802.11b** }
Parameter Description	*radio-id*: specifies the IDs of the radios assigned with the frequency band. The value ranges from 1 to 96. **802.11a**: specifies the 5 GHz operating band. **802.11b**: specifies the 2.4 GHz operating band.
Defaults	A single-band AP (radio 1) supports the 2.4 GHz frequency band. For a dual-band AP, radio 1 supports the 2.4 GHz frequency band, and radio 2 supports the 5 GHz frequency band.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring the RTS Threshold

- Optional.
- On an AC, configure the RTS threshold for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the configured threshold.

Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: specifies the value of the RTS threshold. The value ranges from 257 to 2347, in the unit of bytes. *radio-id*: specifies the IDs of the radios assigned with the RTS threshold. The value ranges from 1 to 96.

Defaults	The default RTS threshold is 2347.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling Short GI

- Optional.
- On an AC, enable short GI for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use short GI.

Command	**short-gi enable radio** *radio-id* **chan-width** { **20** | **40** | **80** |**160** }
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with short GI. The value ranges from 1 to 96. **20**: specifies the 20 MHz bandwidth. **40**: specifies the 40 MHz bandwidth. **80**: specifies the 80 MHz bandwidth. **160**: specifies the 160 MHz bandwidth.
Defaults	By default, 20Mbps, and 40Mbps at 2.4GHz radio are enabled. 20Mbps, 40Mbps, 80Mbps and 160Mbps at 5.8GHz radio are enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring the Preamble Type

- Optional.
- On an AC, configure the preamble type for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to use the configured preamble type.

Command	**preamble** { **long** | **short** } **radio** *radio-id*
Parameter Description	**long**: indicates that APs transmit only the frames with long preambles. **short**: indicates that APs can transmit the frames with short or long preambles. *radio-id*: specifies the IDs of the radios assigned with the preamble type. The value ranges from 1 to 96.
Defaults	By default, the short preamble type is supported.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.

Configuring the Short Slot Time

- Optional.
- On an AC, configure the short slot time for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to enable the short slot time feature.

Command	**short-slot-time radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios assigned with the short slot time. The value ranges from 1 to 96.
Defaults	By default, the short slot time function is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling TSC Update

- Optional.
- On an AC, enable TSC update for specified APs. Then the AC assigns the settings to the APs to instruct the AP to enable TSC update.

Command	**update-key-tsc enable**
Parameter Description	N/A
Defaults	By default, TSC update is disabled.
Command Mode	AP configuration mode or AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Maximum Distance of Wireless Transmission Between APs and the Peer End

- Optional.
- On an AC, configure the maximum distance of wireless transmission between APs and the peer end for specified APs. Then the AC assigns the settings to the APs to instruct the AP radios to send and receive packets according to the maximum distance.

Command	**peer-distance** *val* **radio** *radio-id*
Parameter Description	*val*: specifies the maximum wireless transmission distance allowed by APs. The value ranges from 1000 to 25000, in the unit of m. *radio-id*: specifies the IDs of the radios assigned with the maximum wireless transmission distance. The value ranges from 1 to 96.

Defaults	By default, the maximum wireless transmission distance is 1000 m.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration is supported only by certain APs.Perform the configuration only when the actual maximum distance of wireless transmission between APs and the peer end is greater than 1000 m. You can set the distance to a large value but do not set it to a value smaller than the actual distance.

Configure MIMO for Multi Users

- Optional.
- After this command is configured, the AC will deliver the configuration to the AP to enable the MU-MIMO function on the AP.

Command	**mu-mimo enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 96.
Defaults	If the radio does not support the mu-mimo function, the AC does not support it by default. If the radio supports the mu-mimo function and it is enabled on the AP by default, it is enabled on the AC by default. If the radio supports the mu-mimo function and it is disabled on the AP by default, it is disabled on the AC by default.
Command Mode	AP configuration mode all-AP configuration mode AP group configuration mode
Configuration Usage Guide	N/A

Enabling the OFDMA Function for a Radio

- Optional.
- After this command is configured, 802.11ax STAs can transmit data by using OFDMA.

Command	**ofdma enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio. The value ranges from **1** to **96**.
Defaults	OFDMA is enabled by default.
Command Mode	AP configuration mode, all-AP configuration mode, and AP group configuration mode
Usage Guide	N/A

Configuring Radio Parameters(Power, Channel, Antenna Type)

- Optional.
- After this command is configured,, the AC will change the radio type or optimize the power, channel, antenna configuration and deliver the configuration to the AP.

Command	**radio-optimize** [{ **802.11a** | **802.11b** } { **802.11a** | **802.11b** }]
Parameter Description	**802.11a**: specifies the 5 GHz operating band. **802.11b**: specifies the 2.4 GHz operating band.
Defaults	This function is disabled by default.
Command Mode	AP configuration mode
Configuration Usage Guide	This command cannot be configured in all-AP configuration mode. If the target AP is offline, you can optimize the radio configuration but cannot change the radio type. If you want to change the radio type, please run the **radio-type** command. The optimized configuration will be saved and take effect next time when the AP goes online. If the target AP is online, you can optimize the radio configuration and change the radio type. You can also optimize the current radio configuration without changing the radio type. If the AP does not support this function, radio configuration will not be changed. If the AP supports this function, radio configuration will be optimized immediately and this command will be saved.

Configuring Channel Switching

- Optional.
- After this command is configured, the AC will switch the two channels on the same radio.

Command	**channel-switch** *radio-id1 radio-id2*
Parameter Description	*radio-id1*: Specifies the first radio ID. *radio-id2*: Specifies the second radio ID.
Defaults	Mcell function is disabled by default.
Command Mode	AP configuration mode
Configuration Usage Guide	This command cannot be configured in all-AP configuration mode. This command cannot be configured for offline APs. This command must be configured after the third radio is enabled for user access. This command is not saved. After configuration, the channels are switched and then saved.

Enabling mcell Function

- Optional.
- After this command is configured, the AP reception sensitivity will be reduced.

Command	**mcell enable radio** *radio-id*
Parameter Description	*radio-id*: specifies the radio ID, in the range from 1 to 96.
Defaults	Mcell function is disabled by default.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Verification

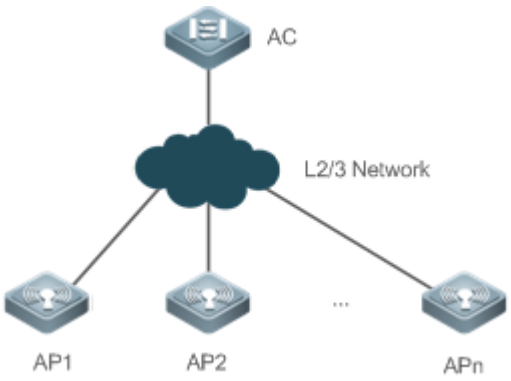
- Run **show ap-config running** *ap-name* to display the parameter settings of STA access control.

Configuration Example

Configuring AP RF Parameters

Scenario

Figure 4-4



In Figure 4-4 an AC is connected to fit APs. On the AC, configure the RF parameters for AP1 according to the following steps:

1. Set the global country code to CNCN.
2. Configure support for CN on the AC.
3. Enable A-MPDU for radio 1 of AP1.
4. Set the maximum 802.11n MCS index value to 15 for radio 1 of AP1.
5. Set the maximum 802.11ac MCS index value to 19 for radio 1 of AP1.
6. Set the maximum 802.11ax MCS index value to 21 for radio 2 of AP1.
7. Set the antenna selection masks of the transmit type and receive type to 7 and 5 respectively for radio 1 of AP1.
8. Enable usage of external antennas and disable usage of internal antennas for radio 1 of AP1.
9. Enable directional antenna on AP1.
10. Set the beacon frame transmission period to 200 ms for radio 1 of AP1.
11. Configure the "CN" country code for radio 1 of AP1.
12. Assign channel 11 to radio 1 of AP1.
13. Assign the 20 MHz bandwidth to radio 1 of AP1.
14. Enable short GI for radio 1 of AP1 in 20 MHz.
15. Enable the protection mode for radio 1 of AP1.
16. Configure 3.2us guard interval for 802.11ax packets on radio2 of AP1.
17. Configure the short preamble type for radio 1 of AP1.
18. Configure the short slot time for radio 1 of AP1.
19. Assign channel 149 to radio 2 of AP1.
20. Assign the 40 MHz bandwidth to radio 2 of AP1.
21. Enable radio 2 of AP1.
22. Set the fragmentation threshold to 2346 bytes for radio 2 of AP1.
23. Set the percent of transmit power to 100% for radio 2 of AP1.
24. Set the RTS threshold to 2347 bytes for radio 2 of AP1.
25. Enables TSC update for AP1.

	26. Set the maximum distance of wireless transmission between APs and the peer end to 3000 m for radio 1 of AP1. 27. Enable MU-MIMO onAP1 Radio 2
	28. Set the maximum distance of wireless transmission between APs and the peer end to 3000mradio 1 of AP1. 29. Enable MU-MIMO for radio 2 of AP1. 30. Enable ofdma for radio 2 of AP1.
Configuration Steps	● On the AC, configure the RF parameters for AP1.

```
Ruijie# configure terminal
Ruijie(config)# country-code CN
Ruijie(config)# ac-controller
Ruijie(config-ac)# country CN
Ruijie(config-ac)# exit
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# 802.11n a-mpdu enable radio 1
Ruijie(config-ap)# 802.11n mcs support 15 radio 1
Ruijie(config-ap)# 802.11ac mcs support 19 radio 1
Ruijie(config-ap)# 802.11ac mcs support 21 radio 2
Ruijie(config-ap)# antenna transmit 7 radio 1
Ruijie(config-ap)# antenna receive 5 radio 1
Ruijie(config-ap)# external-antenna enable radio 1
Ruijie(config-ap)# country CN radio 1
Ruijie(config-ap)# antenna type direction
Ruijie(config-ap)# beacon period 200 radio 1
Ruijie(config-ap)# country CN radio 1
Ruijie(config-ap)# channel 11 radio 1
Ruijie(config-ap)# chan-width 20 radio 1
Ruijie(config-ap)# short-gi enable radio 1 chan-width 20
Ruijie(config-ap)# green-field enable radio 1
Ruijie(config-ap)# preamble short radio 1
Ruijie(config-ap)# short-slot-time radio 1

Ruijie(config-ap)# channel 149 radio 2
Ruijie(config-ap)# chan-width 40 radio 2
Ruijie(config-ap)# enable-radio 2
Ruijie(config-ap)# fragment-threshold 2346 radio 2
Ruijie(config-ap)# power local 100 radio 2
Ruijie(config-ap)# rts-threshold 2347 radio 2
Ruijie(config-ap)# update-key-tsc enable
```

	Ruijie(config-ap)# peer-distance 3000 radio 1 Ruijie(config-ap)# ofdma enable radio 2
	Ruijie(config-ap)# ofdma enable radio 2
Verification	● Run **show ap-config running** *ap-name* to display the RF parameter settings of AP1.
	Ruijie(config)# show ap-config running AP1 ! ap-config AP1 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 802.11ac mcs support 19 radio 1 update-key-tsc enable short-gi enable radio 1 chan-width 20 green-field enable radio 1 station-role root-ap radio 1 station-role root-ap radio 2 chan-width 40 radio 2 antenna receive 5 radio 1 external-antenna enable radio 1 channel 11 radio 1 channel 149 radio 2 beacon period 200 radio 1 power local 100 radio 2 peer-distance 3000 radio 1

	!

4.4.3 Configuring Data Rate Control Parameters

Configuration Effect

- Configure the data rate control parameters for fit APs centrally for easier configuration management.

Configuration Steps

Configuring the Data Rate Set Supported by 802.11a STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11a STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11a STAs.

Command	**802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }
Parameter Description	**6**: specifies the 6 Mbps data rate. **9**: specifies the 9 Mbps data rate. **12**: specifies the 12 Mbps data rate. **18**: specifies the 18 Mbps data rate. **24**: specifies the 24 Mbps data rate. **36**: specifies the 36 Mbps data rate. **48**: specifies the 48 Mbps data rate. **54**: specifies the 54 Mbps data rate. **disabled**: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.
Defaults	Support for the 6 Mbps, 12 Mbps, and 24 Mbps data rates is mandatory, whereas support for the 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command Mode	AC configuration mode/AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Data Rate Set Supported by 802.11b STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11b STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11b STAs.

Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported**}
Parameter Description	**1**: specifies the 1 Mbps data rate. **2**: specifies the 2 Mbps data rate. **5**: specifies the 5.5 Mbps data rate. **11**: specifies the 11 Mbps data rate.

	disabled: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.
Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory.
Command Mode	AC configuration mode/AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Data Rate Set Supported by 802.11g STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11g STAs. Then the AC assigns the settings to all the APs to instruct the APs to apply the configured data rate set to 802.11g STAs.

Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported**}
Parameter Description	**1**: specifies the 1 Mbps data rate. **2**: specifies the 2 Mbps data rate. **5**: specifies the 5.5 Mbps data rate. **6**: specifies the 6 Mbps data rate. **9**: specifies the 9 Mbps data rate. **11**: specifies the 11 Mbps data rate. **12**: specifies the 12 Mbps data rate. **18**: specifies the 18 Mbps data rate. **24**: specifies the 24 Mbps data rate. **36**: specifies the 36 Mbps data rate. **48**: specifies the 48 Mbps data rate. **54**: specifies the 54 Mbps data rate. **disabled**: indicates that the data rate set is not supported. **mandatory**: indicates that support for the data rate set is mandatory. **supported**: indicates that support for the data rate set is optional.
Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory, whereas support for the 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command Mode	AC configuration mode/AP configuration mode/AP group configuration mode
Configuration Usage Guide	N/A

Configuring the Multicast Rate

- Optional.

- On an AC, configure the multicast rate for a WLAN. Then the AC assigns the settings to all the APs on the WLAN to instruct the APs to apply the configured multicast rate within the range of the WLAN.

Command	**mcast-rate** *mcas-num*
Parameter Description	*mcast-num*: specifies the WLAN multicast rate. The 1 Mbps, 6 Mbps, 11 Mbps, 24 Mbps, and 54 Mbps options are available.
Defaults	The default multicast rate is 24 Mbps.
Command Mode	WLAN configuration mode
Configuration Usage Guide	N/A

Configuring the Beacon Frame Transmission Rate

- Optional.
- On an AC, configure the beacon frame transmission rate for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit beacon frames according to the configured rate.

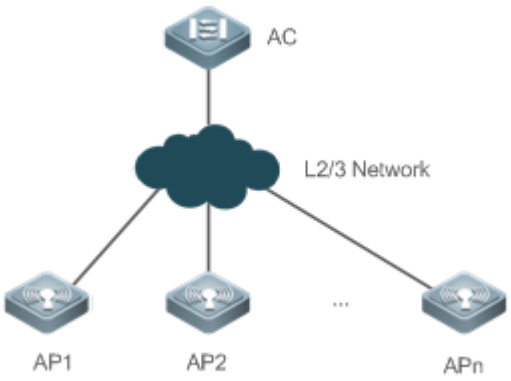
Command	**beacon rate** *rate-Mbps* **radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*rate_Mbps*: specifies the rate at which beacon frames are transmitted. *radio-id*: specifies the IDs of the radios assigned with the beacon frame transmission rate. The value ranges from 1 to 96. *802.11b*: indicates that the beacon frame transmission rate is assigned to all the radios in 2.4 GHz. *802.11a*: indicates that the beacon frame transmission rate is assigned to all the radios in 5.8 GHz.
Defaults	By default, no beacon frame transmission rate is configured.
Command Mode	AP configuration mode
Configuration Usage Guide	1. Do not configure a beacon frame transmission rate that is disabled in the data rate set settings. 2. Because the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps rates are not supported in 5 GHz, do not set the beacon frame transmission rate to any of the preceding values for the radios in 5 GHz. 3. If you select **802.11b**, the beacon frame transmission rate is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

Verification

- Run **show running** to display the parameter settings of data rate control.

Configuration Example

Configuring Data Rate Control Parameters

Scenario **Figure 4-5**	 In Figure 4-5, an AC is connected to fit APs. On the AC, configure the data rate control parameters according to the following steps: 1. Disable the 6 Mbps rate for 802.11a STAs. 2. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11b STAs. 3. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g STAs. 4. Set the multicast rate for WLAN1 to 54 Mbps.
	On the AC, configure the data rate control parameters for AP1 according to the following step: 1. Configure the beacon frame transmission rate for radio 1 of AP1.
Configuration Steps	● On the AC, configure the data rate control parameters.
	`Ruijie# configure terminal` `Ruijie(config)# ac-controller` `Ruijie(config-ac)# 802.11a network rate 6 disabled` `Ruijie(config-ac)# 802.11b network rate 1 disabled` `Ruijie(config-ac)# 802.11b network rate 2 disabled` `Ruijie(config-ac)# 802.11b network rate 5 disabled` `Ruijie(config-ac)# 802.11g network rate 1 disabled` `Ruijie(config-ac)# 802.11g network rate 2 disabled` `Ruijie(config-ac)# 802.11g network rate 5 disabled` `Ruijie(config-ac)# exit` `Ruijie(config)# wlan-config 1` `Ruijie(config-wlan)# mcast-rate 54`
	● On the AC, configure the beacon frame transmission rate for AP1.

	Ruijie# configure terminal Ruijie(config)# ap-config AP1 Ruijie(config-ap)# beacon rate 12.0 radio 1
Verification	● Run **show running-config** to display the parameter settings of data rate control.
	Ruijie# show running-config ... ! wlan-config 1 ss enable-broad-ssid mcast-rate 54 ! ... ! ac-controller country CN 802.11g network rate 1 disabled 802.11g network rate 2 disabled 802.11g network rate 5 disabled 802.11g network rate 11 mandatory 802.11g network rate 6 supported 802.11g network rate 9 supported 802.11g network rate 12 supported 802.11g network rate 18 supported 802.11g network rate 24 supported 802.11g network rate 36 supported 802.11g network rate 48 supported 802.11g network rate 54 supported 802.11b network rate 1 disabled 802.11b network rate 2 disabled 802.11b network rate 5 disabled

	802.11b network rate 11 mandatory 802.11a network rate 6 disabled 802.11a network rate 9 supported 802.11a network rate 12 mandatory 802.11a network rate 18 supported 802.11a network rate 24 mandatory 802.11a network rate 36 supported 802.11a network rate 48 supported 802.11a network rate 54 supported ! ...
	● Run **show ap-config running** *ap-name* to display the beacon frame transmission rate settings of AP1.
	Ruijie(config)# show ap-config running AP1 ! ap-config AP1 channel 11 radio 1 channel 149 radio 2 beacon period 200 radio 1 beacon rate 12.0 radio 1 power local 100 radio 2 !

4.4.4 Configuring Power-Save Parameters

Configuration Effect

- Configure the power-save parameters for fit APs centrally for easier configuration management.

Configuration Steps

↘ Configuring the DTIM Period

- Optional.
- The power saving effect is improved if the DTIM period is set to a large value, but the delay for downstream multicast packets is increased.

Command	**beacon dtim-period** *period-num* **radio** *radio-id*
Parameter Description	*period-num*: specifies the DTIM period. The value ranges from 1 to 255. The unit is expressed as the period of one beacon frame. *radio-id*: specifies the IDs of the radios assigned with the DTIM period. The value ranges from 1 to 96.
Defaults	The unit of the DTIM period is expressed as the period of one beacon frame.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling or Disabling U-APSD Power Saving

- Optional.
- Enable U-APSD power saving to reduce the delay of the services with high real-time requirements during the power management process. The transmission of radio signals can be disabled during most of the time to extends the battery life.

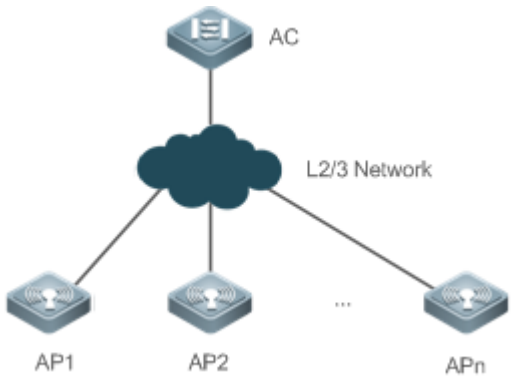
Command	**apsd** { **enable | disable** } **radio** *radio-id*
Parameter Description	**enable**: enables U-APSD power saving. **disable**: disables U-APSD power saving. *radio-id*: specifies the IDs of the radios enabled with U-APSD power saving. The value ranges from 1 to 96.
Defaults	By default, U-APSD power saving is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display the power-save parameter settings.

Configuration Example

Configuring Power-Save Parameters

Scenario **Figure 4-6**	
Configuration Steps	● On the AC, set the DTIM period to 3 for radio 1 of AP1. ● On the AC, enable U-APSD power saving for radio 1 of AP1.
	Ruijie#configure terminal Ruijie(config)#ap-config AP0001 Ruijie(config-ap)#beacon dtim-period 3 radio 1 Ruijie(config-ap)#apsd enable radio 1
Verification	● Run **show ap-config running** *ap-name* to display the power-save parameter settings of AP1.
	Ruijie(config)# show ap-config running AP1 ! ap-config AP1 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 update-key-tsc enable short-gi enable radio 1 chan-width 20 green-field enable radio 1 station-role root-ap radio 1 station-role root-ap radio 2 chan-width 40 radio 2 antenna receive 5 radio 1 channel 11 radio 1 channel 149 radio 2 beacon period 200 radio 1

	beacon dtim-period 3 radio 1 power local 100 radio 2 !

4.4.5 Enabling Link Integrity Detection

Configuration Effect

- Enable link integrity detection.

Configuration Steps

Enabling Link Integrity Detection

- (Mandatory) Run **link-check enable** to enable link integrity detection.

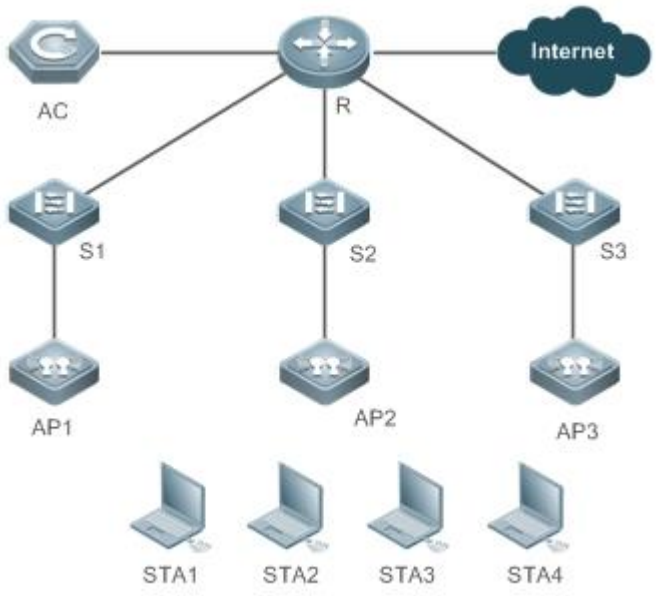
Command	**link-check enable**
Parameter Description	N/A
Defaults	By default, link integrity detection is disabled.
Command Mode	Global configuration mode
Configuration Usage Guide	By default, link integrity detection is disabled.

Verification

- Run **show running-config** to display the configuration status of link integrity detection.

Configuration Example

Enabling Link Integrity Detection

Scenario **Figure 4-7**	 In Figure 4-7, an AC is connected to fit APs. Enable link integrity detection according to the following step: 1. Enable link integrity detection.
Configuration Steps	● Enable link integrity detection on the AC.
	`Ruijie# configure terminal` `Ruijie(config)# link-check enable`
Verification	● Run **show running-config** to display the configuration status of link integrity detection.
	`Ruijie(config)# show running-config` `.....` `link-check enable` `.....`

4.4.6 Configuring E-Bag Parameters

Configuration Effect

- Configure the E-bag parameters for APs and radios for easier configuration management.

Configuration Steps

↘ Configuring the A-MPDU Software Retransmission Times

- Optional.

- On an AC, configure the A-MPDU software retransmission times for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit A-MPDU packets according to the configured times.
- The greater the retransmission times, the lower the probability of sub-frame loss. If packets are retransmitted frequently, the burden on the air interface is increased, which affects the real-time transmission of packets on the air interface. You can increase the retransmission times if you need to avoid packet loss when there is a high probability of sub-frame loss.

Command	**ampdu-retries** *times* **radio** *radio-id*
Parameter Description	*times*: specifies the A-MPDU software retransmission times. The value ranges from 1 to 10. *radio-id*: specifies the IDs of the radios assigned with the A-MPDU software retransmission times. The value ranges from 1 to 96.
Defaults	By default, the A-MPDU software retransmission times is 10.
Command Mode	AP configuration mode
Configuration Usage Guide	The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode. The configuration is supported only by certain APs.

Enabling or Disabling RTS Protection for A-MPDU Packets

- Optional.
- On an AC, enable RTS protection for A-MPDU packets for specified APs. Then the AC assigns the settings to the APs to instruct the APs to transmit A-MPDU packets using RTS protection.
- Enable RTS protection only when the resource waste on the air interface caused by hidden nodes is greater than the resource consumption of RTS interaction on the air interface.

Command	**ampdu-rts radio** {*radio-id* | [*802.11b* | *802.11a*]}
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with RTS protection. The value ranges from 1 to 96. *802.11b*: indicates that RTS protection is enabled for all the radios in 2.4 GHz. *802.11a*: indicates that RTS protection is enabled for all the radios in 5.8 GHz.
Defaults	By default, RTS protection for A-PMDU packets is disabled.
Command Mode	AP configuration mode
Configuration Usage Guide	If you select **802.11b**, RTS protection for A-PMDU packets is enabled for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz. The configuration takes effect only when the AP radios operate in 802.11n or 802.11ac mode.

Configuring the Single-Time Received Ethernet Packet Quantity for APs

- Optional.
- By default, the single-time received Ethernet packet quantity varies with different APs.
- On an AC, configure the single-time received Ethernet packet quantity for specified APs. Then the AC assigns the settings to the APs to instruct the APs to limit the number of Ethernet packets received at a single time according to the settings.

Increasing Ethernet packet reception can improve network performance but may reduce APs' ability to handle key packets in real time. You can reduce Ethernet packet reception when the requirements for performance are not high but user concurrency and real-time packet handling are demanded. In this case, it is recommended that the single-time received Ethernet packet quantity be set to 25.

Command	**eth-schd** *limit*
Parameter Description	*limit*: specifies the number of Ethernet packets received at a single time. The value ranges from 1 to 256.
Defaults	By default, the single-time received Ethernet packet quantity varies with different APs.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling or Disabling LDPC

- Optional.
- On an AC, enable LDPC for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets using LDPC.
- LDPC improves the coding reliability and gains. It also greatly reduces the probability of information loss during transmission in frequencies with serious noise interference. However, a small number of STAs are not compatible with LDPC, and enabling LDPC will result in packet loss.

Command	**ldpc radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with LDPC. The value ranges from 1 to 96.
Defaults	By default, LDPC is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Enabling or Disabling Transmit/Receive STBC

- Optional.
- On an AC, enable transmit/receive STBC for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets using STBC.
- STBC improves the reliability of data transmission. Some STAs may not be compatible with STBC.

Command	**stbc radio** *radio-id*
Parameter Description	*radio-id*: specifies the IDs of the radios enabled with STBC. The value ranges from 1 to 96.

Defaults	By default, STBC is enabled.
Command Mode	AP configuration mode
Configuration Usage Guide	N/A

Configuring E-bag Network Optimization in One-Click Mode

- Optional.
- Run **ebag** in AP configuration mode to quickly configure E-bag network optimization in one-click mode.
- The AP320, AP330, and AP3220 are optimized in the following aspects:

- Packet handling optimization on wired ports: **eth-schd 25**
- Optimization of wireless aggregate packet retransmission: **ampdu-retries 2**
- WiFox is disabled.

- The AP530 is optimized in the following aspects:

- By default, radios 1 and 2 use the sta-idle-time 1800 settings.
- Radio 1 optimization: The 1 Mbps, 2 Mbps, and 5.5 Mbps mandatory rates are disabled for 802.11b/g STAs, and the 11 Mbps and 24 Mbps rates are configured as mandatory rates for 802.11g STAs. RTS protection for A-MPDU packets is enabled.

- On an AC, configure E-bag network optimization for specified APs. Then the AC assigns the settings to the APs to instruct the APs to send and receive packets according to the settings.

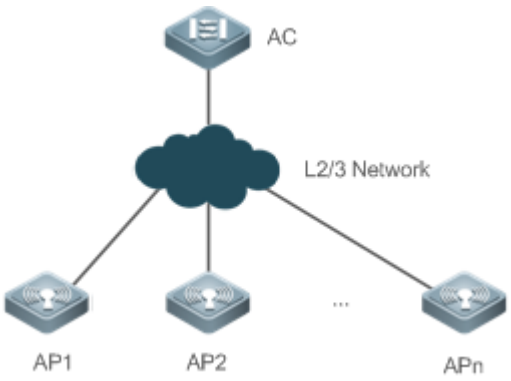
Command	**ebag**
Parameter Description	N/A
Defaults	No default settings are available.
Command Mode	AP configuration mode
Configuration Usage Guide	Use this command only when E-bag is configured. If E-bag is not configured, do not use this command unless necessary.

Verification

- Run **show ap-config running** *ap-name* to display the E-bag parameter settings.

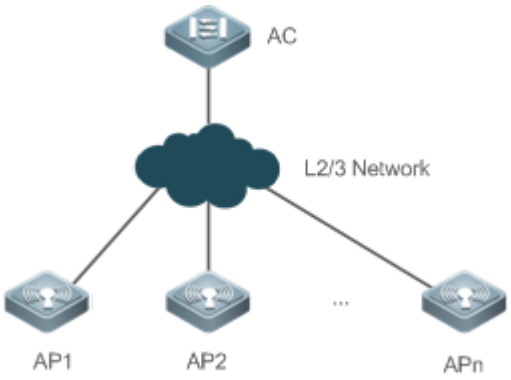
Configuration Example

Configuring E-Bag Parameters

Scenario **Figure 4-8**	 In Figure 4-8, an AC is connected to APs. On the AC, configure the E-bag parameters for AP1 according to the following steps: 1. Set the A-MPDU software retransmission times to 3 for radio 1 of AP1. 2. Enable RTS protection for A-MPDU packets for radio 1 of AP1. 3. Set the single-time received Ethernet packet quantity to 100 for AP1. 4. Disable LDPC for radio 1 of AP1. 5. Disable transmit/receive STBC for radio 1 of AP1.
Configuration Steps	● On the AC, configure the RF parameters for AP1.
	`Ruijie# configure terminal` `Ruijie(config)# ap-config AP1` `Ruijie(config-ap)# ampdu-retries 3 radio 1` `Ruijie(config-ap)# ampdu-rts radio 1` `Ruijie(config-ap)# eth-schd 100` `Ruijie(config-ap)# no ldpc radio 1` `Ruijie(config-ap)# no stbc radio 1`
Verification	● Run **show ap-config running** *ap-name* to display the E-bag parameter settings of AP1.
	`Ruijie(config)# show ap-config running AP1` `!` `ap-config AP1` ` ap-mac 00d0.f801.0528` `channel 11 radio 1` ` no 11acsupport enable radio 2`

	ampdu-retries 3 radio 1 ampdu-rts radio 1 no stbc radio 1 no ldpc radio 1 eth-schd 100 wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2 !

Configuring E-bag Network Optimization in One-Click Mode

Scenario **Figure 4-9**	 In Figure 4-9, an AC is connected to fit APs. AP1 is configured with E-bag settings. On the AC, configure E-bag network optimization for AP1 in one-click mode.
Configuration Steps	● On the AC, configure E-bag network optimization for AP1 in one-click mode.
	Ruijie# configure terminal Ruijie(config)# ap-config AP1 Ruijie(config-ap)# ebag
Verification	● Run **show ap-config running** *ap-name* to display the E-bag parameter settings of AP1.
	Ruijie(config)# show ap-config running AP1 ! ap-config AP1 ap-mac 00d0.f801.0528

```
channel 11 radio 1
no 11acsupport enable radio 2
ampdu-retries 2 radio 1
ampdu-retries 2 radio 2
eth-schd 25
ebag
wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1
wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2
!
```

4.4.7 Configuring WLANs in One-Click Mode

Configuration Effect

- Configure WLANs quickly on devices with zero configurations in one-click mode. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Configuration Steps

↘ Configuring WLANs in One-Click Mode

- Optional.
- Run **autowifi** in configuration mode to configure WLANs in one-click mode, thus realizing fast configuration of wireless networks. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

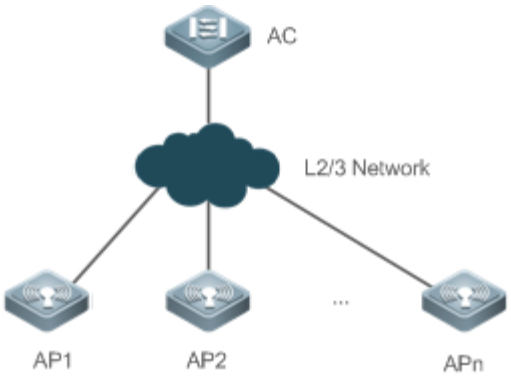
Command	**autowifi**
Parameter Description	N/A
Defaults	No default settings are available.
Command Mode	AC global configuration mode
Configuration Usage Guide	The one-click WLAN configuration feature allows you to perform fast configuration on devices with zero configurations. The one-click WLAN configuration feature helps the land survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Verification

- Run **show running** to display the one-click WLAN configuration.

Configuration Example

Configuring WLANs in One-Click Mode

Scenario **Figure 4-10**	 In Figure 4-10, an AC is connected to fit APs. Configure WLANs in one-click mode on the AC.
Configuration Steps	● Configure WLANs in one-click mode on the AC.
	`Ruijie# configure terminal` `Ruijie(config)# autowifi`
Verification	● Run **show running** to display the one-click WLAN configuration.
	`Ruijie(config)# show running` `!` `wlan-config 1 autowifi_1234` `!` `ap-group default` ` interface-mapping 1 2 ap-wlan-id 1` `!` `ap-config all` ` fair-schedule` `!` `ac-controller` ` 802.11g network rate 1 mandatory` ` 802.11g network rate 2 mandatory`

```
 802.11g network rate 5 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 11 mandatory
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 mandatory
 802.11b network rate 2 mandatory
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 mandatory
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
ip dhcp pool web_ap_pool_1
 option 138 ip 88.88.88.88
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool web_sta_pool_1
 network 192.168.2.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.2.1
```

```
!
link-check disable
!
vlan 1
!
vlan 2
!
interface Loopback 0
 ip address 88.88.88.88 255.255.255.255
!
interface VLAN 1
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
!
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii autowifi
!
```

4.4.8 Managing the Operating Frequency Band When Power Supply Is Insufficient

Configuration Effect

When the AP power supply mode is negotiated to 15.4 W, the AP can work only in 2.4 GHz or 5 GHz. This configuration enables the AP to switch the operating frequency band (2.4 GHz or 5 GHz).

Notes

- None

Configuration Steps

- Optional.

- After this command is configured, the AC delivers the configuration to an AP to notify the AP of the operating frequency band when power supply is insufficient.

Command	**hap-poe enable radio** { **802.11a** | **802.11b** }
Parameter Description	**802.11a**: Indicates the 5 GHz band. **802.11b**: Indicates the 2.4 GHz band.
Defaults	The operating frequency band is selected based on the AP capability value by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	

Verification

Run the **show ap-config running** *ap-name* command to display configurations in AP configuration mode and run the **show running** command to display configurations in AP group configuration mode and all-AP configuration mode.

Configuration Example

Switching to 5 GHz When AP Power Supply Is Insufficient

Configuration Steps

The following example switches the operating frequency band to 5 GHz on the AC when power supply to AP1 is insufficient.

```
Ruijie# configure terminal
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# hap-poe enable radio 802.11a
```

Verification

Run the **show ap-config running** *ap-name* command to display configuration of a specific AP.

```
Ruijie(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528
 hap-poe enable radio 802.11a
!
```

4.5 Monitoring

Displaying

Description	Command
Displays the link information of wireless STAs.	**linktest**
Displays the AP list that maps the 802.11a or 802.11b network on an AC.	**show ac-config** { **802.11a** | **802.11b** } **summary**
Displays the antenna feeder status of all APs.	**show antenna all**
Displays the antenna feeder status of an AP.	**show antenna single** *ap-name*
Displays the radio information of all APs.	**show ap-config radio**
Displays the radio information of an AP.	**show ap-config radio ap-name** *ap-name*
Displays the configuration information of an AP radio.	**show ap-config radio** *radio-id* **config** *ap-name*
Displays the status information of an AP radio.	**show ap-config radio** *radio-id* **status** *ap-name*
Displays the radio list of an AP.	**show ap-config radio status** *ap-name*
Displays the radio information of all APs.	**show ap-config summary radio**
Displays the STA information mapped to a MAC address.	**show client details** *sta-mac*

5 Configuring WLAN WBS FWD

5.1 Overview

WLAN Basic Service-Forward Mode (WBS-FWD) is used to control the forwarding mode of packets on access points (APs). Ruijie access controllers (ACs) and APs build communications through the Control and Provisioning of Wireless Access Points (CAPWAP) channel. The AP forwards data packets in one of the following modes:

- Centralized forwarding mode: An AP encapsulates received wireless data into 802.3 frames, and sends the packets through the CAPWAP channel to the AC, which forwards the packets. When an AC receives the data packets, it sends the packets through the CAPWAP channel to the AP, which transforms the format of the packets into 802.11 frame format and sends them to the STAs.
- Local forwarding mode: An AP encapsulates received wireless data into 802.3 frames and performs Layer-2/Layer-3 forwarding, namely, the packets will be forwarded directly by the AP.

You can configure the forwarding mode for all the APs on the entire wireless local area network (WLAN), or you can specify the forwarding mode for a specified virtual local area network (VLAN), IP address, or a packet of a certain type. You can configure the AP forwarding mode based on different scenarios such as the AP load and centralized management, so that packets of different types are forwarded as required.

5.2 Applications

Application	Description
Centralized Forwarding Mode	All branch APs are managed by an AC and all packets are forwarded by the AC.
Local Forwarding Mode	All branch APs are managed by an AC, and the packets are forwarded by the AP locally.

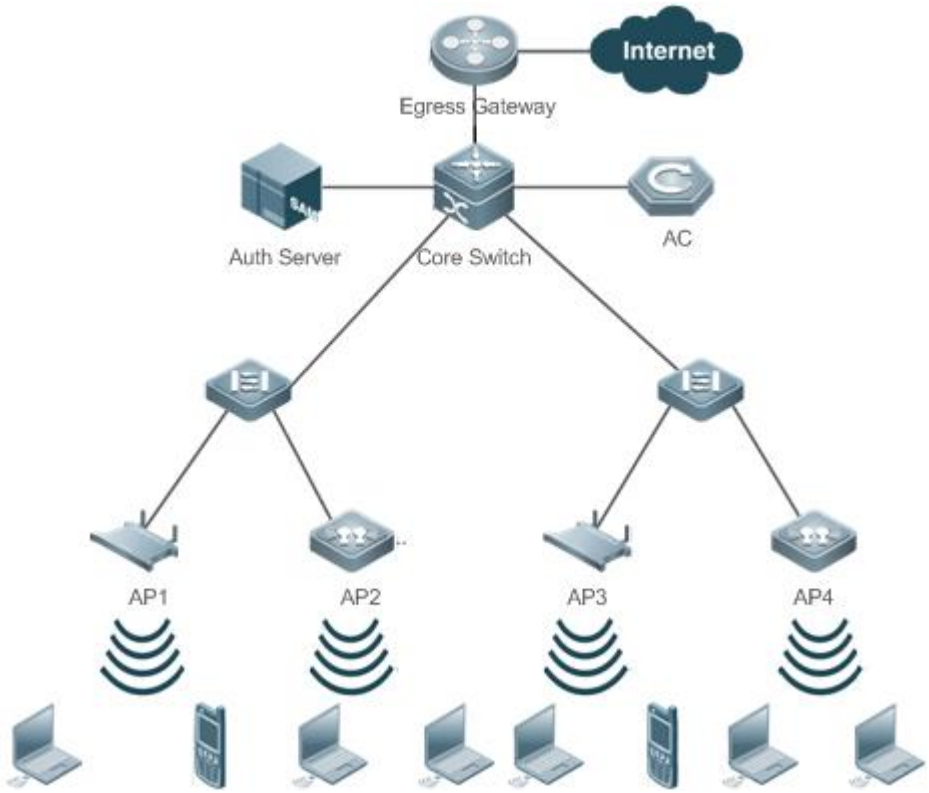
5.2.1 Centralized Forwarding Mode

Scenario

Centralized forwarding mode is applied to the following scenarios:

- All APs and the AC are within the same VLAN with sufficient bandwidth.
- The AC has high forwarding performance.
- The network egress is unified.

Figure 5-1



Deployment

- On the AC, configure centralized forwarding mode for APs.

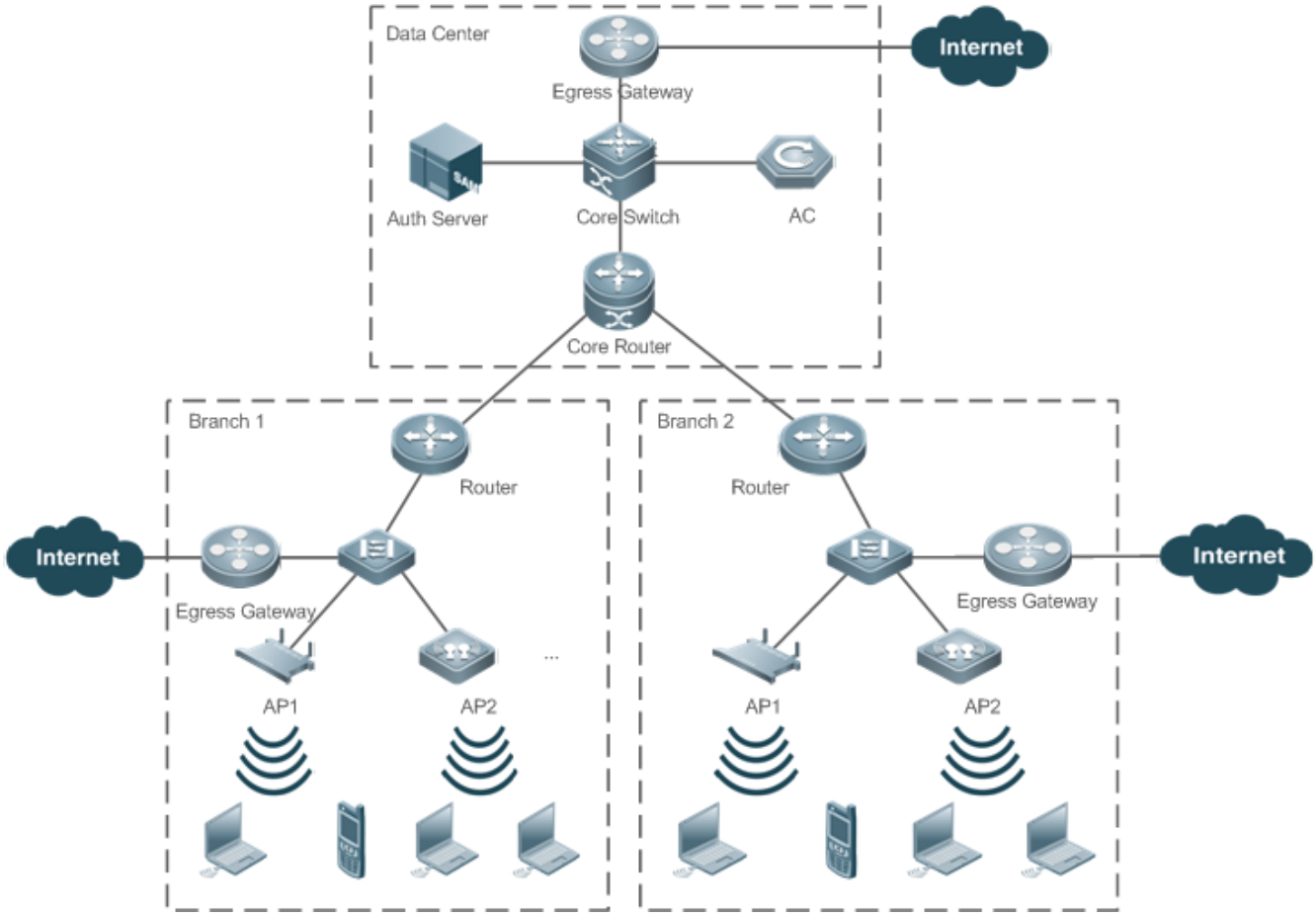
5.2.2 Local Forwarding Mode

Scenario

Local forwarding mode is applied to the following scenarios:

- APs are deployed in different branches and are managed by the AC in the headquarters.
- The bandwidth of the links between branches and the headquarter is low.
- Each branch has an independent egress.

Figure 5-2



Deployment

- On the AC, configure local forwarding mode for APs.
- On the AC, configure centralized forwarding mode for Dynamic Host Configuration Protocol (DHCP).

5.3 Features

Basic Concepts

Centralized Forwarding Mode and Local Forwarding Mode

Ruijie ACs and APs build communications through the CAPWAP channel. The AP forwards data packets in one of the following modes:

- Centralized forwarding mode: An AP encapsulates received wireless data into 802.3 frames, and sends the packets through the CAPWAP channel to the AC, which forwards the packets. When an AC receives the data packets, it sends the packets through the CAPWAP channel to the AP, which transforms the format of the packets into 802.11 frame format

and sends them to the STAs. In this case, packets are forwarded by an AC, which is convenient for centralized control and maintenance on the AC. On the other hand, it will burden the AC and require higher performance of the AC.

- Local forwarding mode: An AP encapsulates received wireless data into 802.3 frames and performs Layer-2/Layer-3 forwarding, namely, the packets will be forwarded directly by the AP. This mode poses little burden on the AC but cannot achieve centralized control and maintenance.

Comparison between the Two Forwarding Modes:

Forwarding Mode	Advantage	Disadvantage	Scenario
Centralized forwarding mode	Centralized control and maintenance on an AC; flexible service expansion	High requirement for AC performance	High AC performance, high bandwidth of links between APs and AC, few APs under an AC, and flexible service
Local forwarding mode	Low requirement for AC performance	No centralized control and maintenance	Low AC performance, low bandwidth of links between APs and AC, and many APs under an AC

Overview

Feature	Description
Configuring the Forwarding Mode of an AP	Specifies the forwarding mode of different packets on an AP.
Configuring the Forwarding Mode of an AC	Specifies the forwarding mode of different packets on an AC.

5.3.1 Configuring the Forwarding Mode of an AP

You can configure the AP forwarding mode based on different scenarios such as the AP load and centralized management, so that packets of different types are forwarded as required.

Working Principle

Forwarding Mode

There are two kinds of forwarding modes, namely, centralized forwarding mode and local forwarding mode. When an AP receives a wireless packet, it forwards the packet based on the configured mode.

You can configure the packet forwarding mode for an AP on an AC.

Configuring a Forwarding Mode

Ruijie products support the following forwarding modes:

- WLAN-based forwarding mode: Forwards the packets on all APs based on the forwarding mode (centralized forwarding mode or local forwarding mode) specified for the WLAN.

- VLAN-based forwarding mode: Forwards the packets on APs within a specified VLAN of a WLAN based on the forwarding mode (centralized forwarding mode or local forwarding mode) specified for the VLAN.
- IP-based forwarding mode: Forwards the packets of a specified destination IP address in local forwarding mode.
- DHCP-based centralized forwarding mode: Forwards all DHCP packets in centralized forwarding mode. If this function is enabled, all DHCP packets will be sent in centralized forwarding mode.

Priorities of Different Forwarding Modes

Ruijie products support the preceding four forwarding modes. These modes can be configured at the same time and their priorities are ranked as follows (in descending order):

1. DHCP-based centralized forwarding mode
2. IP-based forwarding mode
3. VLAN-based forwarding mode
4. WLAN-based forwarding mode

After a wireless packet is received by an AP, the packet will be forwarded based on the priority of the forwarding mode. If a mode of high priority is detected, the packet will be forwarded in this mode; if not, the packet will be forwarded in the default centralized forwarding mode.

For example:

1. If DHCP forwarding mode is configured, all the DHCP packets will be forwarded in centralized mode.
2. For a non-DHCP packet, if its IP address is specified for local forwarding, the packet will be forwarded in local forwarding mode. If not, Step 3 will be performed.
3. If the VLAN where the packet belongs is configured with a forwarding mode, the packet will be forwarded in this mode. If not, Step 4 will be performed.
4. If the WLAN where the packet belongs is configured with a forwarding mode, the packet will be forwarded in this mode. If not, Step 5 will be performed.
5. The packet will be forwarded in the default centralized forwarding mode.

5.3.2 Configuring the Forwarding Mode of an AC

You can configure the forwarding mode for an AC based on the load of the entire wireless network, unified management requirement, and the actual service environment. The AC adjusts, based on the configured forwarding mode, internal parameters to better adapt to the current service environment.

Working Principle

Forwarding Mode

There are hybrid forwarding mode and local forwarding mode. In AC hybrid forwarding mode, WLANs support both the centralized forwarding mode and local forwarding mode, that is, some WLANs use centralized forwarding while other WLANs

use local forwarding. In AC local forwarding mode, WLANs support only local forwarding mode (including local authentication forwarding mode).

Forwarding Mode Settings

You can configure the forwarding mode for an AC.

5.4 Configuration

Configuration	Description and Command	
Configuring WLAN-based Forwarding Mode	(Mandatory) It is used to specify the forwarding mode for the entire WLAN.	
	tunnel	Specifies the forwarding mode for the entire WLAN.
Configuring VLAN-based Forwarding Mode	(Optional) Specifies the forwarding mode for a specified VLAN of a WLAN.	
	tunnel local wlan	Specifies local forwarding as the forwarding mode for a specified VLAN of a WLAN.
	tunnel 8023 wlan	Specifies centralized forwarding as the forwarding mode for a specified VLAN of a WLAN.
Configuring IP-based Forwarding Mode	(Optional) It is used to specify local forwarding as the forwarding mode for a specified IP address.	
	local fw ip	Forwards all packets of a specified IP address in local forwarding mode.
Configuring DHCP-based Forwarding Mode	(Optional) It is used to specify centralized forwarding as the forwarding mode for DHCP packets.	
	central dhcp enable	Forwards all DHCP packets in a WLAN in centralized forwarding mode.
Configuring AC Forwarding Mode	(Optional) It is used to specify AC forwarding mode.	
	tunnel-mode	Specifies the AC forwarding mode

5.4.1 Configuring WLAN-based Forwarding Mode

Configuration Effect

- Specify a forwarding mode for the entire WLAN, including local forwarding mode, centralized forwarding mode, and local authentication forwarding mode.

Notes

- The **tunnel local-auth** command takes effect only when remote intelligent perception technology (RIPT) is enabled.

Configuration Steps

- Mandatory.
- In WLAN configuration mode on an AC, configure the forwarding mode for the entire WLAN as local forwarding mode, centralized forwarding mode, or local authentication forwarding mode.
- The default forwarding mode is centralized forwarding.
- Configure the forwarding mode before applying the WLAN template to a specified AP group. Otherwise, the configuration will not take effect.

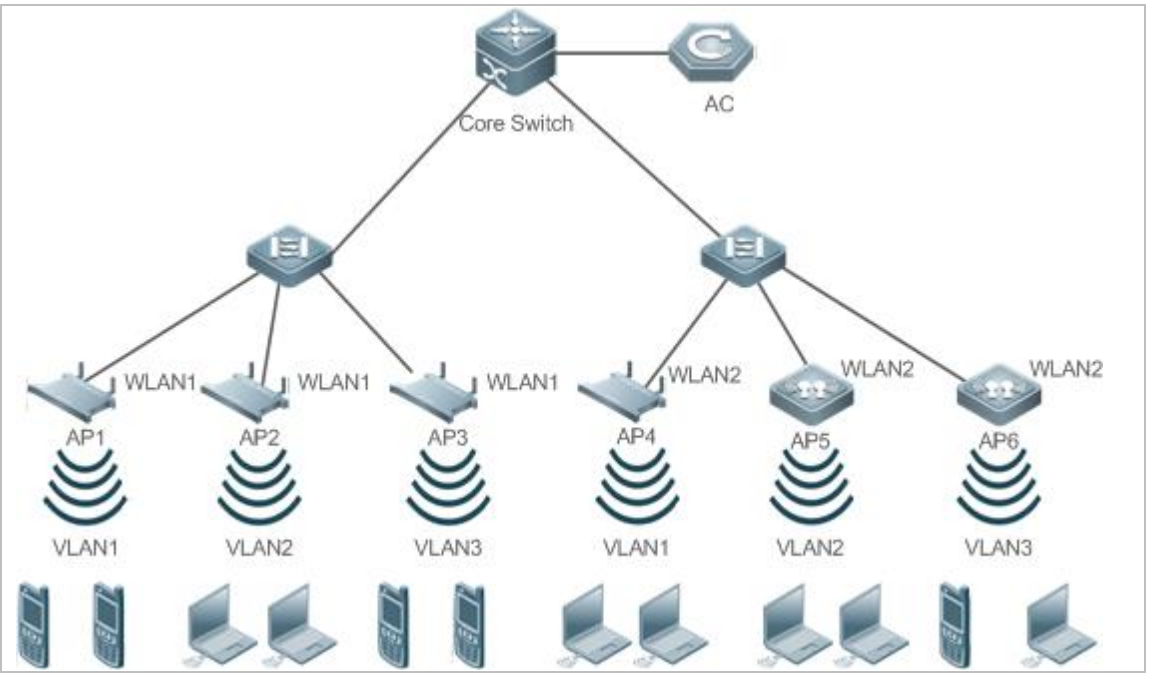
Command	**tunnel** { **8023** | **local** | **local-auth** }
Parameter Description	**8023**: An AP encapsulates received wireless data into a 802.3 frame and forwards the packet to an AC. **local**: An AP forwards packets locally. **local-auth**: Indicates local forwarding mode. An AP forwards packets locally, and STAs are authenticated on the AP.
Defaults	The default forwarding mode is centralized forwarding.
Command Mode	WLAN configuration mode
Usage Guide	The **local-auth** command takes effect only when RIPT is enabled.

Verification

- Verify the WLAN configuration.

Configuration Example

Configuring the Forwarding Mode for All Packets in a WLAN

Scenario **Figure 5-3**	

	• With low bandwidth, WLAN 1 contains AP 1, AP 2 and AP 3 for the access of mobile phones. WLAN 1 is configured with centralized forwarding mode. • With high bandwidth. WLAN 2 contains AP 4, AP 5, and AP 6 for the access of PCs. WLAN 2 is configured with local forwarding mode.
Configuration Steps	• Enter WLAN configuration mode. • Configure the forwarding mode of the WLAN.
WLAN1	`Ruijie(config)#wlan-config 1` `Ruijie(config-wlan)#tunnel local`
WLAN2	`Ruijie(config)#wlan-config 2` `Ruijie(config-wlan)#tunnel 8023`
Verification	N/A

5.4.2 Configuring VLAN-based Forwarding Mode

Configuration Effect

- Specify the forwarding mode for a specified VLAN of a WLAN.

Notes

- You can specify the forwarding mode for the entire WLAN in WLAN-based forwarding mode, or you can specify the forwarding mode for a specified VLAN of the WLAN in VLAN-based forwarding mode.
- As VLAN-based forwarding mode prevails over WLAN-based forwarding mode, if both of these modes are configured, the packets in the specified VLAN will be forwarded in VLAN-based forwarding mode, and the others will be forwarded in WLAN-based forwarding mode.
- Configure either local forwarding or centralized forwarding for a VLAN. The two cannot be both configured.
- The VLAN can be an interface-based VLAN, MAC-based VLAN, or authentication-based VLAN.

Configuration Steps

↘ Configuring the Forwarding Mode of a WLAN

- (Optional) If the forwarding mode of a specified VLAN of a WLAN is different from the other VLANs, specify a forwarding mode for this VLAN.
- The default forwarding mode is the same as the WLAN-based forwarding mode.
- In AP group configuration mode on an AC, run **tunnel local wlan** [*wlan-id*] **vlan** [*vlan-id*] to specify local forwarding mode for a specified VLAN.

- In AP group configuration mode on an AC, run **tunnel 8023 wlan** [*wlan-id*] **vlan** [*vlan-id*] to specify centralized forwarding mode for a specified VLAN.

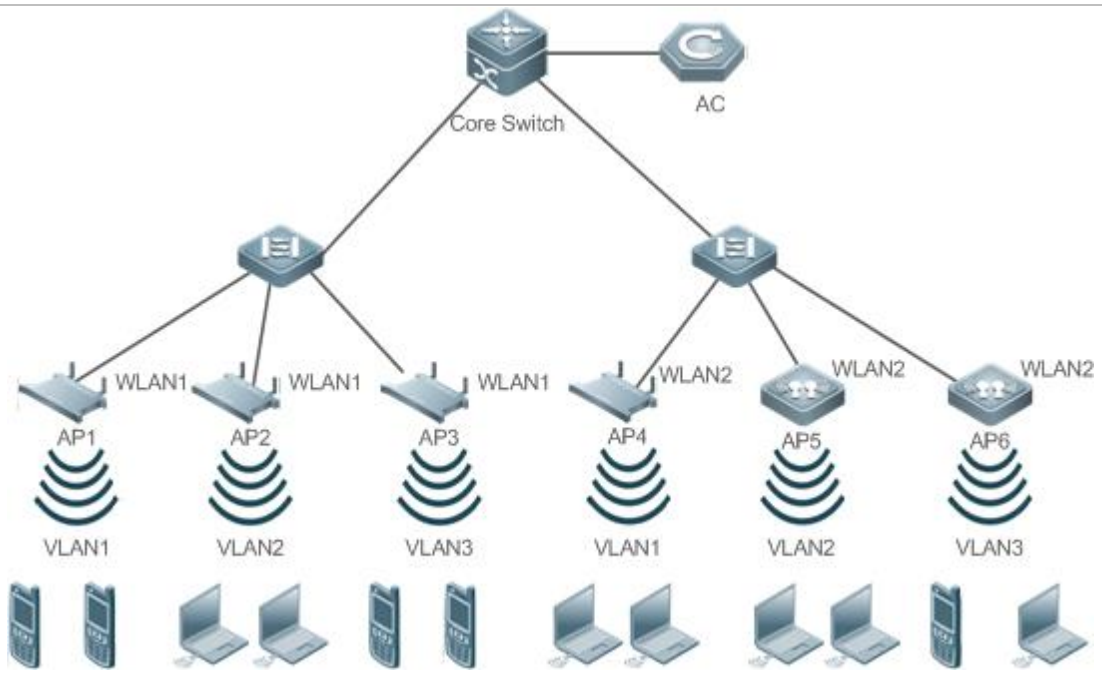
Command	**tunnel local wlan** [*wlan-id*] **vlan** [*vlan-id*]
Parameter Description	*wlan-id*: Indicates the WLAN. The WLAN must have been created. The value ranges from 1 to 4,094. *vlan-id*: Indicates the VLAN. The VLAN must have been created. The value ranges from 1 to 4,094.
Defaults	By default, no VLAN is specified. The forwarding mode is the same as that configured by the **tunnel** command.
Command Mode	ap-group configuration mode
Usage Guide	In WLAN configuration mode, you can run the **tunnel 8023** command to specify centralized forwarding mode for the entire WLAN, or you can run **tunnel local wlan** to specify local forwarding mode for a specified VLAN on the WLAN.

Command	**tunnel 8023 wlan** [*wlan-id*] **vlan** [*vlan-id*]
Parameter Description	*wlan-id*: Indicates the WLAN. The WLAN must have been created. The value ranges from 1 to 4,094. *vlan-id*: Indicates the VLAN. The VLAN must have been created. The value ranges from 1 to 4,094.
Defaults	By default, no VLAN is specified. The forwarding mode is the same as that configured by the **tunnel** command.
Command Mode	ap-group configuration mode
Usage Guide	In WLAN configuration mode, you can run the **tunnel local** command to specify local forwarding mode for the entire WLAN, or you can run the **tunnel local wlan** command to specify centralized forwarding mode for a specified VLAN.

Configuration Example

Configuring the Forwarding Mode of a Specified VLAN on a WLAN

Scenario **Figure 5-4**	

	 ● WLAN 1 contains AP 1, AP 2 and AP 3 which belong to VLAN 1, VLAN 2 and VLAN 3 respectively. Among them, VLAN1 and VLAN 3 are used for the access of mobile phones while VLAN 2 for PCs which require high bandwidth. Therefore, WLAN 1 is configured with centralized forwarding mode while VLAN 2 is configured with local forwarding mode. ● WLAN 2 contains AP 4, AP 5 and AP 6 which belong to VLAN 1, VLAN 2 and VLAN 3 respectively. Among them, VLAN1 and VLAN 2 are used for the access of PCs while VLAN 3 for mobile phones which require low bandwidth. Therefore, WLAN 2 is configured with local forwarding mode while VLAN 3 is configured with centralized forwarding mode.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode of the WLAN. ● Specify a forwarding mode for the specified VLAN on the WLAN.
WLAN1	`Ruijie(config)#wlan-config 1` `Ruijie(config-wlan)#tunnel 8023` `Ruijie(config-wlan)#exit` `Ruijie(config)#ap-group default` `Ruijie(config-ap-group)#tunnel local wlan 1 vlan 2`
WLAN2	`Ruijie(config)#wlan-config 2` `Ruijie(config-wlan)#tunnel local` `Ruijie(config-wlan)#exit` `Ruijie(config)#ap-group default`

	Ruijie(config-ap-group)#tunnel 8023 wlan 2 vlan 3
Verification	N/A

5.4.3 Configuring IP-based Forwarding Mode

Configuration Effect

- Forward the packet of the specified IP address in local forwarding mode.

Notes

- You can configure the forwarding mode of an AP based on a WLAN or VLAN, or you can further configure local forwarding mode for packets of a specified IP address.
- As IP-based forwarding mode prevails over WLAN-based forwarding mode and VLAN-based forwarding mode, if all of these modes are configured, packets of a specified address will be forwarded locally, and the others will be forwarded in WLAN-based forwarding mode or VLAN-based forwarding mode.

Configuration Steps

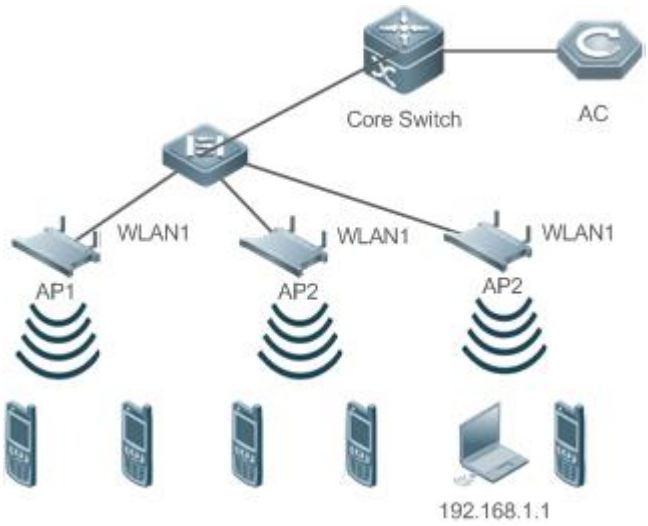
↘ Configuring IP-based Forwarding Mode

- (Optional) You can configure local forwarding mode for packets of a specified IP address.
- In AC configuration mode on an AC, specify local forwarding for a specified IP address.
- If IP-based forwarding is not configured, packets are forwarded based on WLAN or VLAN. If IP-based forwarding is configured, packets of a specified IP address are forwarded locally.

Command	**local fw ip** [*ip address*]
Parameter Description	*ip address*: Indicates the IP address of an STA.
Defaults	By default, all IP packets are forwarded in WLAN-based forwarding mode.
Command Mode	ac-controller configuration mode
Usage Guide	IP-based forwarding is a kind of flexible forwarding mode.

Configuration Example

↘ Configuring Local Forwarding for Packets of a Specified IP Address

Scenario **Figure 5-5**	 ● WLAN 1 contains AP 1, AP 2 and AP 3 which belong to VLAN 1, VLAN 2 and VLAN 3 respectively. Among them, IP address 192.168.1.1 is used for the access of PCs while the others for mobile phones which require low bandwidth. Therefore, configure local forwarding for IP address 192.168.1.1.
Configuration Steps	● Enter AC configuration mode. ● Specify local forwarding mode for a specified IP address.
AC	`ruijie(config)#ac-controller` `ruijie(config-ac)#local fwip 192.168.1.1`
Verification	N/A

5.4.4 Configuring DHCP-based Forwarding Mode

Configuration Effect

- Forwards all DHCP packets in centralized forwarding mode.

Notes

- As DHCP-based forwarding mode prevails over WLAN-based forwarding mode, VLAN-based forwarding mode, and IP-based forwarding mode, if DHCP-based forwarding mode is configured, all the DHCP packets will be forwarded in centralized mode, and others will be forwarded as configured.
- To facilitate management of the DHCP address pool and simplify the DHCP topology, it is recommended to enable this function.

Configuration Steps

↘ **Configuring DHCP-based Forwarding Mode**

- (Optional) Perform the configuration to assign IP addresses to STAs by the AC..
- If DHCP forwarding mode is not configured, DHCP packets will be forwarded in the same way as general packets based on the forwarding mode configured. If DHCP forwarding mode is configured, DHCP packets will be forwarded in a centralized way.
- Configure the forwarding mode before applying the WLAN template to a specified AP group. Otherwise, the configuration will not take effect.

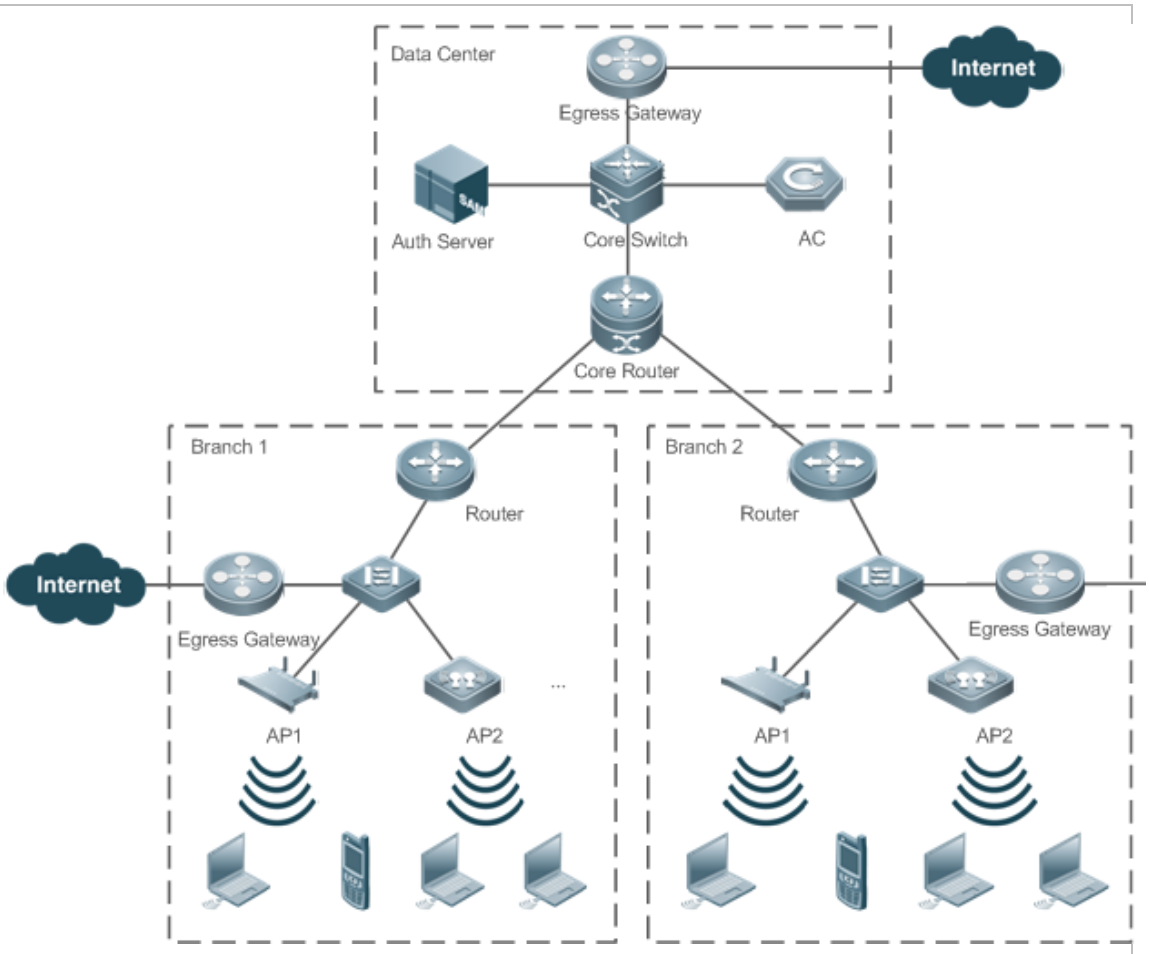
Command	**central dhcp enable**
Parameter Description	N/A
Defaults	By default, all IP packets are forwarded in WLAN-based forwarding mode.
Command Mode	WLAN configuration mode
Usage Guide	To facilitate management of the DHCP address pool and simplify the DHCP topology, it is recommended to enable this function.

Verification

- Verify the WLAN configuration.

Configuration Example

Configuring DHCP Services on an AC

Scenario **Figure 5-6**	 ● APs are deployed in different branches and are managed by the AC in the headquarters. ● The bandwidth of the links between branches and the headquarter is low. ● Each branch has an independent egress. ● IP addresses are assigned by the AC.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode of the WLAN. ● Configure DHCP centralized forwarding mode.
AC	`ruijie(config)#wlan-config 100 ruijie_wlan` `ruijie(config-wlan)#tunnel local` `ruijie(config-wlan)#central dhcp enable`
Verification	N/A

5.4.5 Configuring AC-based Forwarding Mode

Configuration Effect

- Determine the forwarding mode of an AC: hybrid forwarding mode or local forwarding mode. In AC hybrid forwarding mode, WLANs support both the centralized forwarding mode and local forwarding mode, that is, some WLANs use centralized forwarding while other WLANs use local forwarding. In AC local forwarding mode, WLANs support only local forwarding mode (including local authentication forwarding mode).

Configuration Steps

- Optional.
- On an AC, in AC configuration mode, set the forwarding mode of the AC to hybrid forwarding or local forwarding.
- If no forwarding mode is configured for an AC, the AC uses the hybrid forwarding mode by default.
- Save the configuration and restart the device after configuration. Otherwise, the configuration does not take effect.

Command	**tunnel-mode** { **hybrid** | **local** }
Parameter Description	**hybrid**: Indicates the AC hybrid forwarding mode. In this mode, WLANs support the coexistence of centralized forwarding mode and local forwarding mode, that is, some WLANs use centralized forwarding while some WLANs adopt local forwarding. **local**: Indicates the AC local forwarding mode. In this mode, WLANs support only local forwarding mode (including local authentication forwarding mode).
Defaults	The default value is hybrid forwarding mode.
Command Mode	AC configuration mode
Usage Guide	1. The AC forwarding mode switching takes effect only after the configuration is saved and the device is restarted. Mode switching does not trigger device restart and you need to manually restart the device. 2. If the device is restarted after the AC forwarding mode configuration is added to or modified in the **config.text** file, the configuration takes effect only after the device is restarted again. It is invalid to delete the AC forwarding mode configuration from the **config.text** file. 3. The AC forwarding mode configuration is preconfigured in the system, that is, the configuration takes effect after the device is restarted even if the **write** command is not executed. 4. If the tunnel mode is set to **hybrid** for an AC, the AC is explicitly configured to adopt the hybrid forwarding mode. After configuration, the tunnel mode is unchanged when the default configuration is updated due to the AC version upgrade. 5. When an AC switches from hybrid forwarding mode to local forwarding mode, WLANs using centralized forwarding automatically switch to local forwarding mode after the device restart. 6. When an AC switches from local forwarding mode to hybrid forwarding mode, the forwarding mode of WLANs does not change automatically after the device restart. 7. In local forwarding mode, service configurations that need to be supported by centralized forwarding keep unchanged but their functions do not take effect. Such configurations include but are not limited to the broadcast forwarding proportion and token bucket configuration of the data plane, WQoS AC-based rate limit, WIDS AC-based/AC-SSID-based layer-2 isolation, and application identification.

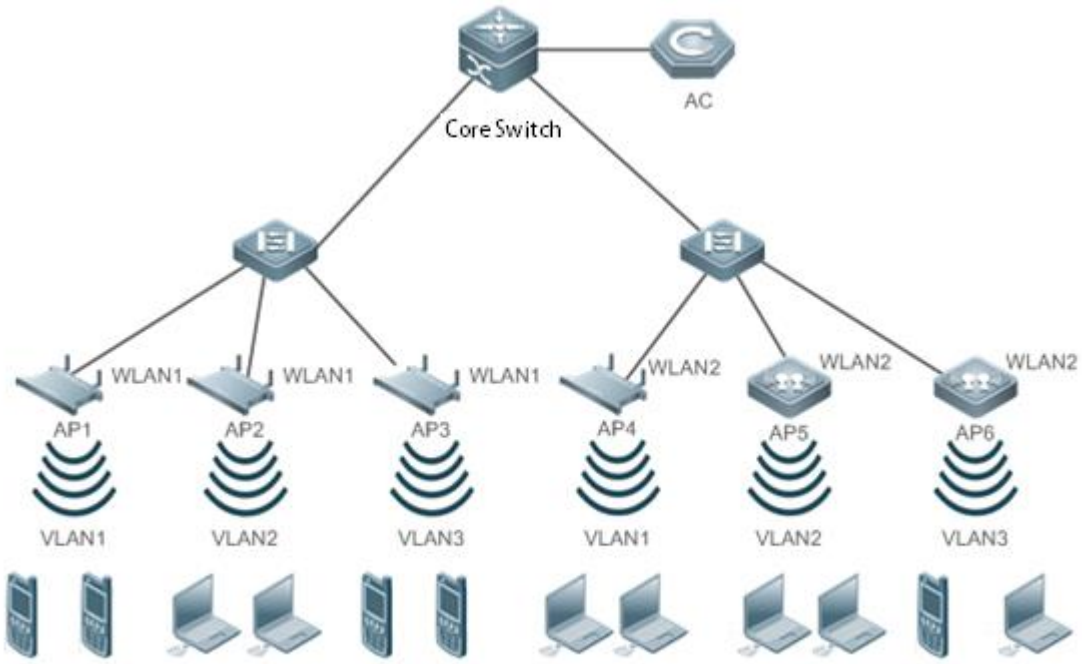
	8. The maximum number of manageable APs and STAs changes accordingly after the AC forwarding mode is changed. 9. The AC forwarding mode does not support default configuration restoration using the reset button.

Verification

- Check the AC configurations.
- Run the **show ac-config** command to display the current effective forwarding mode of the AC.

Configuration Example

Setting the Forwarding Mode of an AC to Local Forwarding

Scenario **Figure 5-7**	 Note: ● The AC is deployed in bypass mode. All STA traffic does not need to pass through the AC. The AC is configured in local forwarding mode so as to manage more APs.
Configuration Steps	● Enter the AC configuration mode. ● Configure the forwarding mode for the AC, save the configuration, and restart the device.
	`Ruijie(config)#ac-controller` `Ruijie(config-ac)#tunnel-mode local` `Ruijie(config-ac)#end` `Ruijie#write`

	Building configuration... [OK] Ruijie#reload Reload system?(Y/N)y
Verification	N/A

5.5 Monitoring

Displaying

Description	Command
Displays the WLAN configuration.	**show wlan-config cb** *wlan-id*
Displays the AC forwarding mode	**show ac-config**

6 Configuring ETH-MNG

6.1 Overview

Wired ports of an AP include WAN ports and LAN ports. The WAN ports are used to connect to the uplink access switches, and the LAN ports exist in some AP products (wall-mounted AP series and i-Share+ AP series) and are used to access wired STAs or other devices and forward data to WAN ports. In the fit AP network architecture, an AP obtains the AC IP address over the WAN port to establish a CAPWAP tunnel, and the AP restricts AC IP address obtaining via DHCP packets over the LAN port. The LAN port cannot be used to establish a CAPWAP tunnel.

6.1.1 Protocols and Standards

- N/A

6.2 Applications

Application	Description
Configuring VLANs on LAN Ports	Configure VLANs on LAN ports to separate APs and wired users.

6.2.1 Configuring VLANs on LAN Ports

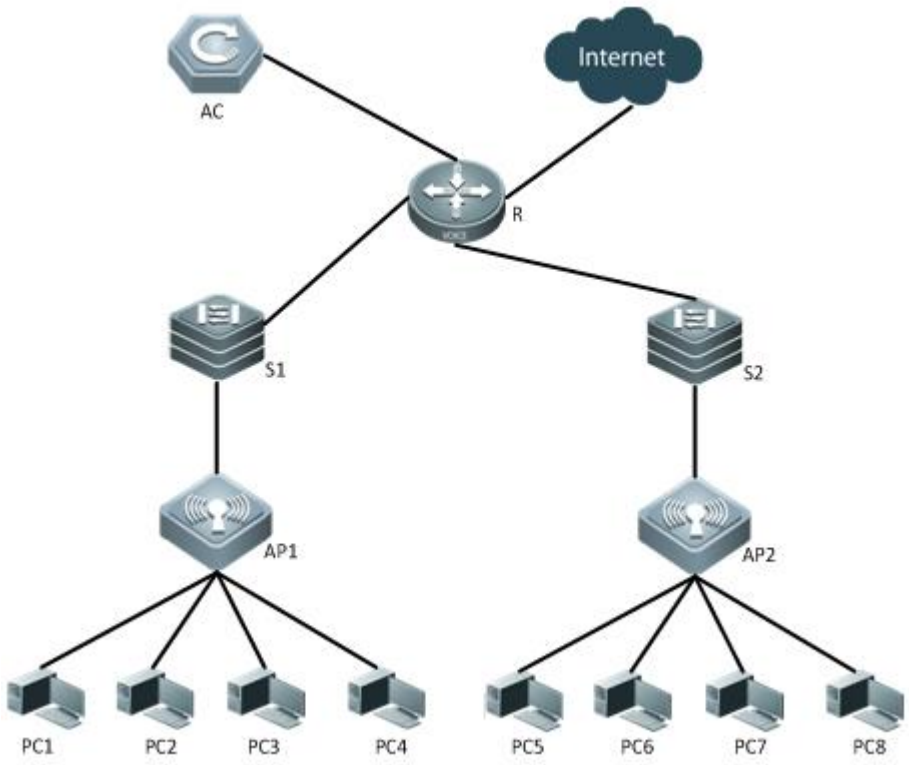
Scenario

Configure VLANs on LAN ports.

In the following figure:

- An AC is connected to the Internet through a router. Two APs (AP1 and AP2) are connected to the router through two switches, and are associated with the AC.
- PC1, PC2, PC3, and PC4 are associated with AP1; PC5, PC6, PC7, and PC8 are associated with AP2. These PCs access the Internet through the AC.

Figure 6-1



R is a network egress router.
S1 and S2 are Layer 2 (L2) switches, and serve as the access devices of the APs.
AP1 is directly connected to S1, and AP2 to S2.

Corresponding Protocols

- The L2 switches provide the access function for the APs.
- The router R is connected to the network formed by the AC and the APs. It is also connected to the PCs and the Internet.
- Configure VLANs on LAN ports.

6.3 Features

Basic Concepts

N/A

Overview

Feature	Description

VLAN Configuration of an AP	Configure the default VLAN of an AP, VLANs on wired ports, and transmission VLANs of iShare+ series.
Maximum LAN Port Bandwidth	Configure the maximum bandwidth of various LAN ports of APs so as to avoid the slow Internet access of wireless users in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.

6.3.1 VLAN Configuration of an AP

Working Principle

An AP automatically removes the native VLAN tag from frames to be sent to STAs. That is, in local forwarding mode, if the VLAN of an STA is the same as the native VLAN, frames sent to the STA will not carry the native VLAN tag, and the access switch determines the VLAN to which the STA belongs. The default VLAN of the AP is VLAN 1. The default VLAN of the AP, VLAN of wireless users, and VLAN of wired users can be planned flexibly to ensure that the STAs and AP are in the same VLAN or different VLANs.

iShare+ APs can be deployed in cascading mode, and the transmission VLAN can be configured to ensure that VLAN packets of downlink devices can be forwarded by uplink devices.

6.3.2 LAN port Bandwidth Restriction

Working Principle

The LAN port bandwidth restriction function is used to configure the maximum bandwidth of various LAN ports of APs so as to avoid the slow Internet access of wireless users caused in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.

6.4 Configuration

Configuration	Description and Command	
Configuring the Default VLAN of an AP	⚠ (Optional) It is used to configure the native VLAN of an AP.	
	ap-vlan	Configures the default VLAN of an AP.
Configuring the transmission VLAN	⚠ (Optional) It is used to configure the transmission VLAN of an AP.	
	pass-vlan	Configures the transmission VLAN of an AP.
Configuring the VLAN of AP Wired Users	⚠ (Optional) It is used to configure the VLAN of wired users when the AP provides an Ethernet interface for access of wired users.	
	wired-vlan	Configures the VLAN used by the wired network port.

Configuring the Wired Network Port Status of an AP	⚠ (Optional) It is used to disable wired network ports when the AP provides Ethernet ports for access of wired users.	
	wired-interface	Disables wired network ports of an AP.
Configuring the Sub-Interface of the WAN Interface on the AP	⚠ (Optional) It is used to configure the sub-interface of the WAN interface on the AP.	
	ap-subif	Configures the sub-interface of the WAN interface on the AP.
Configuring the Maximum Bandwidth of LAN ports	⚠ (Optional) It is used to configure the maximum bandwidth of LAN ports of APs.	
	wired-rate *value*	Configures Rate LAN ports on the AP.
Configuring Port Mode Switching of an AP	⚠ (Optional) It is used to configure port mode switching of an AP.	
	switch port-mode	Configures port mode switching of an AP.

6.4.1 Configuring the Default VLAN of an AP

Configuration Effect

The AP automatically removes the TAG from a frame that contains the native VLAN before forwarding the frame. That is, in local forwarding mode, when the VLAN of the user is the same as the native VLAN, the frame of the user does not contain the TAG when forwarded, and the access switch determines the VLAN to which the user belongs.

Notes

- After this command is executed, an online AP will go offline and then the connection will be set up again.
- When a wireless distribution system (WDS) is deployed, the same AP-VLAN must be planned for the ROOT-BRIDGE and NONROOT-BRIDGE devices; otherwise, the NONROOT-BRIDGE devices cannot share the same address pool with the ROOT-BRIDGE devices or the NONROOT-BRIDGE devices cannot even forward packets properly.
- This command needs to be configured only in the following case: In local forwarding mode, STAs and an AP belong to a same subnet and VLANs have been configured for the STAs and the AP. This command is not required in other cases.
- If the static DHCP address pool is configured, and the client ID is specified to use Bridge-Group Virtual Interface (BVI) 1, configuration of this command will change the BVI interface of the AP. In this case, the DHCP server configuration must be modified; otherwise, the address cannot be obtained.
- If the AP uses the PPPoE dial-up mode to obtain the address, the CAPWAP module on the AP will select dialer 1 as the source interface, and the STA traffic will be forwarded without containing the TAG. Therefore, this command is meaningless.

Configuration Steps

↘ Configuring the Default VLAN of an AP

- Optional.

- When planning of the users' native VLANs is required, you can configure the same VLAN as the default VLAN of an AP and the VLAN of the user. In this way, both the VLAN of the user and the VLAN of the AP are determined by the access switch.

Command	ap-vlan*vlan-id*
Parameter Description	*vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. The default value is 1.
Defaults	1
Command Mode	AP configuration mode or all AP (ap-config all) configuration mode
Usage Guide	The AP automatically removes the TAG from a frame that contains the native VLAN before forwarding the frame. That is, in local forwarding mode, when the VLAN of the user is the same as the native VLAN, the frame of the user does not contain the TAG when forwarded, and the access switch determines the VLAN to which the user belongs.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Setting the VLAN ID of the Native VLAN of AP1 to 20

Configuration Steps	Enter the AP configuration mode on the AC. Set the VLAN ID of the native VLAN of AP1 to 20.
AC	Ruijie(config)# ap-config AP1 Ruijie(config-ap)# ap-vlan20
Verification	Run the **show ap-config running** command to display the location information of AP1.
AC	Ruijie#show ap-config running ! ap-config AP1 ap-vlan 20 !

Common Errors

According to the planning, the native VLAN of the switch is VLAN 20, and all wireless/wired users and APs belong to VLAN 20. The following configurations are incorrect:

On the AC:

```
Ruijie(config)# ap-configAP120
Ruijie(config-ap)# wired-vlan20
Ruijie(config-ap)# exit
Ruijie(config)#wlan-config 1 ssid
Ruijie(config-wlan)#tunnel local
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 1 20 radio 1
```

On the switch:

```
Ruijie(config)#interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)#switchport trunk native vlan 20
```

The configurations here are incorrect because the VLAN of users is different from the native VLAN of APs. Therefore, the uplink packets of APs contain TAG 20 when forwarded, and the access switch transparently forwards VLAN 20 and assigns addresses to users. As the native VLAN of the switch is VLAN 20, the downlink packets do not contain the TAG when forwarded. The Native VLAN of APs is 1 by default. Therefore, the packets cannot be forwarded to users, and the wireless and wired users cannot obtain their addresses.

Either of the following methods can be used to modify the configurations:

Method 1: Change **wired-vlan 20** to **wired-vlan 1** and **interface-mapping 1 20 radio 1** to **interface-mapping 1 1 radio 1**, and the native VLAN of the switch remains unchanged.

Method 2: Add the native VLAN configurations for APs, and other configurations remain unchanged.

On the AC:

```
Ruijie(config)# ap-configAP120
Ruijie(config-ap)# ap-vlan 20
```

6.4.2 Configuring the Transmission VLAN for an AP

Configuration Effect

When the i-Share+ APs are cascaded or a ring network is deployed, configure the transmission VLAN for the master AP, so that STAs associated with different APs can forward packets if they are deployed in different VLANs.

Notes

The transmission VLAN cannot conflict with the VLANs specified by the **interface-mapping**, **ap-vlan**, and **wired-vlan** commands, and cannot be VLAN 2444.

Configuration Steps

Configuring the Transmission VLAN for the AP

- Optional.
- When the i-Share+ APs are cascaded or a ring network is deployed, run this command to configure the transmission VLAN, so that STAs associated with different APs can forward packets if they are deployed in different VLANs.

Command	**pass-vlan** *vlan-range*
Parameter Description	*vlan-range*: indicates the VLAN ID range. Multiple VLAN IDs can be specified. Separate two VLAN IDs by a comma (,) and separate two VLAN ID ranges by a hyphen (-).
Defaults	No VLAN is configured by default.
Command Mode	AP configuration mode
Usage Guide	1. This command can be configured for all APs but takes effect only on the i-Share+ master AP. 2. When this command is run, the transmission VLAN will be created on the i-Share+ master AP, so that the master AP can forward packets based on the transmission VLAN. In addition, the transmission VLAN will be automatically pruned on the downlink port of the master AP, to prevent broadcast and multicast packets of other master APs from being flooded to mini APs connected to the master AP.

Verification

Run the **show ap-config running** command to display the AP configuration.

Configuration Example

Configuring the Transmission VLAN of AP1 to VLAN 20

Configuration Steps	Enter the AP configuration mode of the AC. Configure the transmission VLAN of AP1 to VLAN 20.
AC	`Ruijie(config)# ap-config AP1` `Ruijie(config-ap)# pass-vlan 20`
Verification	Run the **show ap-config running** command to display transmission VLAN.
AC	`Ruijie#show ap-config running` `!` `ap-config AP1` `pass-vlan 20` `!`

Common Errors

N/A

6.4.3 Configuring the VLAN of Wired Users

Configuration Effect

Specify the VLAN of wired users when the AP provides an Ethernet interface for access of wired users.

Notes

- This command can be configured on all APs, but the configurations take effect only on APs that are equipped with the wired network ports.
- If this command does not contain the **port** parameter, the same VLAN is configured for all the wired network ports. When the same VLAN should be configured for four ports, the command without the **port** parameter is configured and displayed.
- In wireless AP mode, the AP implements only the wireless access function, but does not assign addresses to users. In this mode, if the VLAN used by the wired network port is configured the same as the VLAN of the AP, the VLAN of the packets sent over the wired network port will be determined by the access switch, instead of the VLAN specified in this command. If the packets sent over the wired network port must contain the TAG when forwarded, the native VLAN of the access switch cannot be the same as the VLAN of the wired network port; otherwise, the packets cannot be forwarded to the wired network port.
- In wireless routing mode, the AP can assign addresses to users. In this mode, wired users obtain IP addresses from the DHCP address pool, and the VLAN of the interface of the address pool must be the same as the VLAN specified in this command.
- When the configurations of the wired network port are automatically saved on the AP and the VLAN of the wired network port is different from the native VLAN of the AP, the AP cannot obtain the IP address of the LAN interface on the AP after the AP is restarted, and management cannot be implemented through the wired network port. In this case, the RESET key of the AP can be pressed and held to restore the factory settings.

Configuration Steps

↘ Configuring the Access VLAN of the AP Wired Network Port

- Optional.
- To plan VLANs so that the VLAN of a wired user is different from the VLAN of the AP, run the **wired-vlan** command on the AC.

Command	**wired-vlan** *vlan-id* [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **auto-save**
Parameter Description	*vlan-id*: indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. By default, the VLAN used by the wired network port is the same as the VLAN of the AP. *slot-id*: indicates the slot to which a Mini AP belongs. The value ranges from 1 to 24. **secondary**: applies to the secondary device.

	port-id: indicates the ID of the wired network port. The value ranges from 1 to 4. **auto-save**: indicates that configurations are automatically saved on the AP. After the AP is restarted, the configurations can be restored.
Defaults	By default, the VLAN used by the wired network port is not configured, indicating that this VLAN is the same as the VLAN of the AP.
Command Mode	AP configuration mode, all AP configuration mode, or AP group configuration mode
Usage Guide	The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs. The fit AP is started without being configured, and its configurations are sent from the AC. The auto-save parameter can be configured to enable automatic saving of the wired network port configurations on the AP. In this way, when the AP is disconnected from the AC, the wired network port configurations can be restored after the AP is restarted, and users can still access the network through the wired network port.

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

↘ Configuring VLAN 20 for the Wired Network Port of AP1

Configuration Steps	Enter the AP configuration mode on the AC. Configure VLAN 20 for the wired network port of AP1.
AC	`Ruijie(config)# ap-config AP1` `Ruijie(config-ap)# wired-vlan20`
Verification	Run the **show ap-config running** command to display the configurations of AP1.
AC	`Ruijie#show ap-config running` `!` `ap-config AP1` `wired-vlan 20` `!`

Common Errors

N/A

6.4.4 Configuring the Wired Network Port Status of an AP

Configuration Effect

Enable or disable the wired network port of an AP.

Notes

- This command can be configured on all APs, but the configurations take effect only on APs that are equipped with the wired network ports.
- If this command does not contain the **port** parameter, the same configurations are applied to all the wired network ports. When all the four ports should be disabled, the command without the **port** parameter is configured and displayed.
- After the AP wired network port is disabled and the AP is restarted, management cannot be implemented through the wired network port. In this case, you can press and hold the RESET key of the AP to restore factory settings.

Configuration Steps

↘ Configuring the Wired Network Port Status of an AP

- Optional.
- To enable or disable wired network ports of an AP, run the **wired-interface** command on the AC.

Command	**wired-interface** [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **enable**
Parameter Description	*slot-id*: indicates the slot to which a Mini AP belongs. The value ranges from 1 to 24. **secondary**: applies to the secondary device. *port-id:* indicates the ID of the wired network port. The value ranges from 1 to 4. **enable**: indicates that the specified wired port is enabled.
Defaults	All the wired network ports are enabled by default.
Command Mode	AP configuration mode, all AP configuration mode, or AP group configuration mode
Usage Guide	The wired network ports of APs can be disabled when APs provide the Ethernet ports for access of wired users, but the application scenario does not require access to the wired network or deployment of the wired network is not completed yet. The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs.

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Disabling All Wired Network Ports of AP1

Configuration Steps	Enter the AP configuration mode on the AC. Disable all wired network ports of AP1.
AC	Ruijie(config)# ap-config AP1 Ruijie(config-ap)# no wired-interfaceenable
Verification	Run the **show ap-config running** command to display the configurations of AP1.
AC	Ruijie#show ap-config running ! ap-config AP1 no wired-interfaceenable !

Common Errors

N/A

6.4.5 Configuring the Sub-Interface of the WAN Interface on the AP

Configuration Effect

A wireless AP creates a sub-interface of the WAN interface by default so that the STA data contains the TAG when forwarded. In wireless routing mode that AP can assign addresses to users, the users' gateway is located on the AP, and the related packets do not need to contain the TAG when forwarded. Therefore, the **ap-subif enable** command can be used to delete the sub-interface of the WAN interface on the AP to prevent an address conflict caused by the same gateway address of STAs.

Notes

If the AP obtains the address in PPPoE dial-up mode, the sub-interface of the WAN interface on the AP will be automatically deleted. In dial-up mode, this command cannot be used to configure the sub-interface of the WAN interface on the AP.

Configuration Steps

Configuring the Sub-Interface of the WAN Interface on the AP

- Optional.
- In wireless routing mode, delete the sub-interface of the WAN interface on the AP; otherwise, an address conflict occurs when a large number of packets are forwarded through the sub-interface because the gateway addresses of users are the same.

Command	**ap-subif enable**
Parameter Description	N/A
Defaults	A sub-interface of the WAN interface is created by default.
Command Mode	AP configuration mode or all AP configuration mode
Usage Guide	N/A

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Deleting the Sub Interface of the WAN Interface from AP1

Configuration Steps	Enter the AP configuration mode on the AC. Delete the sub-interface of the WAN interface from AP1.
AC	`Ruijie(config)# ap-config AP1` `Ruijie(config-ap)# no ap-subif enable`
Verification	Run the **show ap-config running** command to display the configurations of AP1.
AC	`Ruijie#show ap-config running` `!` `ap-config AP1` `no ap-subif enable` `!`

Common Errors

N/A

6.4.6 LAN port Bandwidth Restriction

Networking Requirements

- Configure the maximum bandwidth of various LAN ports.

Notes

- N/A

Configuration Steps

Configuring the LAN Port Bandwidth Restriction Function

- The configuration is optional.
- Perform this configuration on the AC or on a fat AP.
- Run the **wired-rate** command to configure the maximum bandwidth of various LAN ports.

Command	**wired-rate** *value* [**port** *port-id*] [**slot** *slot-id* [**secondary**]]
Parameter Description	If no port ID is specified, all ports are configured. If no slot ID is specified for an i-Share+ AP, all LAN ports on all mini APs are configured. The **slot** parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all Mini APs.
Defaults	By default, the maximum bandwidths of various LAN ports are not limited.
Command Mode	AP configuration mode/AP group configuration mode
Usage Guide	N/A

Verification

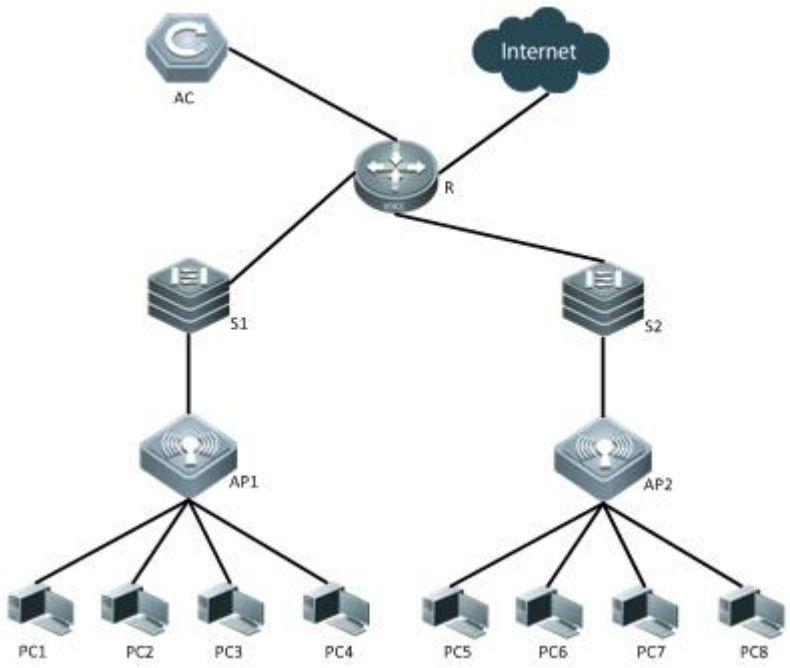
- Run the **show running-config** command to display the configuration about the bandwidth restriction of various LAN ports.

Configuration Example

Configuring LAN Port Bandwidth Restriction

Scenario

Figure 6-2



Suppose the bandwidths of the LAN ports need to be restricted in the fit AP environment, as shown in Figure 6-2.

1. Configure the maximum bandwidth of various LAN ports.

Configuration Steps	● On the AC, set the maximum bandwidth of port 3 on the AP to 30 Mbps.
AC	`Ruijie(config)# ap-config [ap-name]` `Ruijie(config-ap)# wired-rate 30 port 3` ● On the AC, set the maximum bandwidth of port 3 on the group APs to 30 Mbps. `Ruijie(config)# ap-group default` `Ruijie(config-group)#wired-rate 30 port 3` ● On the AC, set the maximum bandwidth of all LAN ports on the group APs to 30 Mbps. `Ruijie(config)# ap-group default` `Ruijie(config-group)#wired-rate 30` ● On the AC, set the maximum bandwidth of port 3 on all APs to 30 Mbps. `Ruijie(config)# ap-config all` `Ruijie(config-ap)# wired-rate 30 port 3` ● On the AC, set the maximum bandwidth of port 3 of slot 3 on the i-Share+ AP to 30 Mbps. `Ruijie(config)# ap-config am5528`

	`Ruijie(config-ap)# wired-rate 30 port 3 slot 3` ● On the AC, set the maximum bandwidth of all LAN ports of slot 3 on the i-Share+ AP to 30 Mbps. `Ruijie(config)# ap-config am5528` `Ruijie(config-ap)# wired-rate 30 slot 3`
AP120-W	● On one AP120-W, set the maximum bandwidth of FastEthernet 0/4 to 40 Mbps. `Ruijie(config)#interface fastEthernet 0/4` `Ruijie(config-if-FastEthernet 0/4)#wired-rate 40`
AP130-W	● On one AP130-W, set the maximum bandwidth of GigabitEthernet 0/4 to 40 Mbps. `Ruijie(config)#interface GigabitEthernet 0/4` `Ruijie(config-if-GigabitEthernet 0/4)#wired-rate 40`
Verification	● On the AC, run the **show ap-config running-config** command to display the configuration.
AC	`Ruijie(config)# show ap-config running-config` `ap-config ap120w-4` `wired-rate 30 port 3`
	● On the AC, run the **show running-config** command to display the configuration.
AC	`Ruijie(config)# show running-config` `ap-group default` `wired-rate 30 port 3`
	● On the AC, run the **show running-config** command to display the configuration.
AC	`Ruijie(config)# show running-config` `ap-group default` `wired-rate 30`
	● On the AC, run the **show running-config** command to display the configuration.

AC	`Ruijie(config)# show running-config` `ap-config all` ` …` ` wired-rate 30 port 3` ` …` `Ruijie(config)# show running-config` `ap-config am5528` ` …` ` wired-rate 30 port 3 slot 3` ` …` `Ruijie(config)# show running-config` `ap-config am5528` ` …` ` wired-rate 30 slot 3` ` …`
	● On the AP, run the **show running-config** command to display the configuration.
AP120-W	`Ruijie(config)# show running-config` `…` `interface FastEthernet 0/4` `wired-rate 40` `…`
AP130-W	`Ruijie(config)# show running-config` `…` `interface GigabitEthernet 0/4` `wired-rate 40` `…`

Common Errors

- N/A

6.4.7 Configuring Port Mode Switching of an AP

Configuration Effect

- The iShare+ product AM5532 can switch among the following three port modes: 4 x 1000M copper ports, 4 x 10G fiber ports, and 2 x 1000M copper ports + 2 x 10G fiber ports.

Notes

- This command takes effect only on the AM5532 and needs to be configured on the AM5532.
- After the switching command is executed, the port mode is automatically saved and the write operation does not need to be executed. However, the device needs to be restarted manually for the configuration to take effect.

Configuration Steps

↘ Configuring Port Mode Switching of an AP

- Optional.
- When the AM5532 is deployed, select the corresponding port mode and connect the network cable.

Command	**switch port-mode** { **copper** | **fiber** | **mixed** }
Parameter Description	**copper**: indicates the mode of 4 x 1000M copper ports. **fiber**: indicates the mode of 4 x 10G fiber ports. **mixed**: indicates the mode of 2 x 1000M copper ports + 2 x 10G fiber ports.
Defaults	The default value is **mixed**, that is, the mode of 2 x 1000M copper ports + 2 x 10G fiber ports.
Command Mode	Privileged EXEC mode
Usage Guide	The uplink ports of the AM5532 support three port modes, that is, 4 x 1000M copper ports, 4 x 10G fiber ports, and 2 x 1000M copper ports + 2 x 10G fiber ports. In the mode of 4 x 1000M copper ports, ports 25 to 28 are used; in the mode of 4 x 10G fiber ports, ports 29 to 32 are used; in the mode of 2 x 1000M copper ports + 2 x 10G fiber ports, ports 27, 28, 31, and 32 are used.

Verification

- Run the **show port-mode** command to display configurations.

Configuration Example

↘ Disabling All Wired Network Ports of AP1

Configuration Steps	● On the AM5532, disable all wired network ports of AP1.
AP	`Ruijie# switch port-mode fiber`
Verification	● Run the **show ap-config running** command to display configurations of AP1.
AC	`Ruijie#show port-mode` `Current port mode:  mixed` `Configure port mode:  fiber`

Common Errors

- N/A

6.5 Monitoring

- N/A

7 Configuring DATA-PLANE

7.1 Overview

The data plane provides broadcast forwarding control functions, including broadcast forwarding weight control and broadcast wireless forwarding control.

Broadcast forwarding weight control means restricting the weights of packet types for broadcast forwarding, so as to prevent STAs from being influenced when a certain type of packets occupy all resources.

Broadcast wireless forwarding control means forwarding only necessary packets to the wireless network, so as to prevent some useless broadcast packets from occupying substantial radio frequency (RF) resources.

- Broadcast forwarding weight control is applicable to all packets to be flooded.
- Broadcast wireless forwarding control is applicable to all packets to be sent to the radio interface.

Protocols and Standards

- N/A

7.2 Applications

Application	Description
Broadcast Forwarding Control	Set up the network with at least one AC and one fit AP.

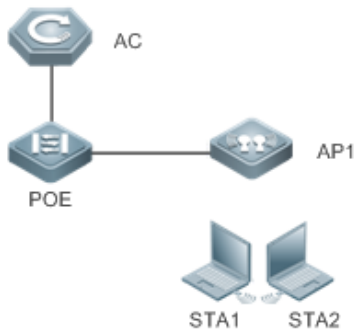
7.2.1 Broadcast Forwarding Control

Scenario

An AC is deployed in the wireless network and enabled with broadcast wireless forwarding control function.

The AC controls the wireless forwarding of broadcast packets, as shown in Figure 7-1.

Figure 7-1



AC: a wireless access controller.
PoE: a gateway switch for the AP.
AP: a wireless access point.
STA1 and STA2: user equipment used as STAs.

Corresponding Protocols

- Enable the broadcast wireless forwarding control function on the AC.

7.3 Features

Basic Concepts

Broadcast Forwarding Weight Control

A network switching device may need to flood broadcast packets, multicast packets, and some unicast packets. A weight can be set for each type of packets to prevent a certain type of broadcast packets from exhausting all broadcast forwarding capabilities, thereby improving STAs' network experience.

Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only necessary broadcast packets to the wireless network, so as to prevent certain broadcast packets from occupying substantial air interface resources and improve the network rates of STAs.

Overview

Feature	Description
Broadcast Forwarding Weight Control	Restricts the weights of packet types for broadcast forwarding, so as to protect RF resources from being occupied by a certain type of packets and thereby guarantee normal forwarding of other packets.
Broadcast Wireless Forwarding Control	Controls whether to forward broadcast packets to the wireless network, so as to prevent useless broadcast packets from occupying substantial RF resources.

7.3.1 Broadcast Forwarding Weight Control

Broadcast forwarding weight control is used to restrict a certain type of packets, so that the ratio of this type of packets is no greater than the specified weight during broadcast forwarding.

Working Principle

The broadcast forwarding weight control function classifies packets at first into unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.

- Classify packets. Packets may be roughly classified into the following types: unicast packets, multicast packets, broadcast packets, unknown multicast packets, and unknown unicast packets.

- Allocate a token bucket to each type of packets, and record the number of packets permitted to pass at this moment.
- According to the configured broadcast forwarding weights, calculate the number of packets permitted to pass within each interval, and adjust the sizes of the token buckets accordingly.
- When a packet arrives, determine the type of the packet and check whether there is any token in the token bucket corresponding to the packet type. If the token bucket contains a token, the packet is permitted to pass; otherwise, the packet is discarded.

7.3.2 Broadcast Wireless Forwarding Control

The broadcast wireless forwarding control function is used to forward only partial packets that affect STAs to the wireless network, so as to prevent useless broadcast packets from occupying substantial air interface resources.

Working Principle

Wireless networks differ from wired networks in performance. In a wireless network, air interface resources are shared by STAs and APs which often becomes a bottleneck for STAs. Meanwhile, they are seized for a long time because broadcast packets are sent at low rates.

In practice, some broadcast packets are useless for STAs. Forwarding these packets to the wireless network will result in fewer air interface resources and worse user experience.

One solution is to classify broadcast packets for forwarding control. Only the packets of specified types are forwarded to the wireless network.

7.4 Configuration

Configuration	Description and Command	
Broadcast Forwarding Weight Control	Optional configuration. Set the weights of packet types for broadcast forwarding.	
	data-plane queue-weight	Configures the weights of packet types for broadcast forwarding on the AC or AP.
	data-plane token	Configures the refresh interval of the broadcast token bucket and bucket-based rate on the AC or AP.
Broadcast Wireless Forwarding Control	Optional configuration. Enable the broadcast wireless forwarding function.	
	data-plane wireless-broadcast	Enables or disables the broadcast wireless forwarding control function on the AC or AP.

7.4.1 Configuring Broadcast Forwarding Weights

Networking Requirements

- You can control the weight of a packet type for forwarding according to actual network conditions, so as to avoid network congestion for sudden traffic spike.

Notes

- N/A

Configuration Steps

Configuring Broadcast Forwarding Weights

- Optional configuration. Run the **data-plane queue-weight** command to configure the broadcast forwarding weights.
- For centralized forwarding, configure this command in the global configuration mode on the AC.
- For local forwarding, configuration this command in the AP configuration mode on the AC.

Command	**data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*
Parameter Description	*unicast-packet-weight*: sets the forwarding weight of unicast packets. The range is from 1 to 100. The default weight is 16. *multicast-packet-weight*: sets the forwarding weight of multicast packets. The range is from 1 to 50. The default weight is 4. *broadcast-packet-weight*: sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default weight is 2. *unknown-multicast-packet-weight*: sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default weight is 1. *unknown-unicast-packet-weight*: sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default weight is 1.
Defaults	Default weights are applied.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Refresh Interval of Broadcast Token Bucket and Bucket-based Rate

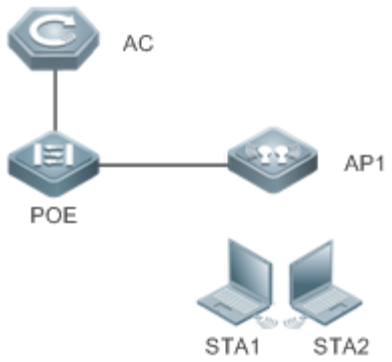
- Optional configuration. Run the **show run** command to display the configuration.
- For centralized forwarding, configure this command in the global configuration mode on the AC.
- For local forwarding, configuration this command in the AP configuration mode on the AC.

Command	**data-plane token** *token-interval token-base-rate*
Parameter Description	*token-interval*: Refresh interval of broadcast token bucket in 10ms. The default interval is 1. *token-base-rate*: Token bucket-based rate. The default rate is 64 for the AC and 5 for the AP.
Defaults	Default parameters are applied.
Command Mode	Global configuration mode
Configuration Usage	Broadcast rate per second = Packet weight × (1s/Refresh Interval) x Token bucket-based rate For example, the broadcast rate per second for the AC = 1 x (1 / 0.01) × 64 = 6400 pps

Configuration Example

Configuring Broadcast Forwarding Weights

Figure 7-2



Configuration Steps	Configure the forwarding weights of packet types for broadcast forwarding in global configuration mode.
AC/AP	`Ruijie#configure terminal` `Ruijie(config)#data-plane queue-weight 100 50 50 25 25` `Ruijie(config)#data-plane token 10 10` `Ruijie(config)#exit`
Verification	Run the **show run** command to display the configuration.

AC/AP	Ruijie#show run ... ! cwmp ! data-plane queue-weight 100 50 50 25 25 data-plane token 10 10 ! ...

Common Errors

- N/A

7.4.2 Configuring Broadcast Wireless Forwarding

Networking Requirements

- Useless broadcast packets are not forwarded to the air interface.

Notes

- N/A

Configuration Steps

↘ Broadcast Forwarding Function

- Optional configuration. By default, the broadcast wireless forwarding function is disabled. Run the data-plane wireless-broadcast command in global configuration mode to enable or disable this function.

Command	**data-plane wireless-broadcast**{ **enable** | **disable** }
Parameter Description	**enable**: permits all broadcast packets to be forwarded to the air interface **disable**: prohibits all broadcast packets from being forwarded to the air interface
Defaults	The broadcast wireless forwarding function is disabled; that is, broadcast packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Configuration Usage	N/A

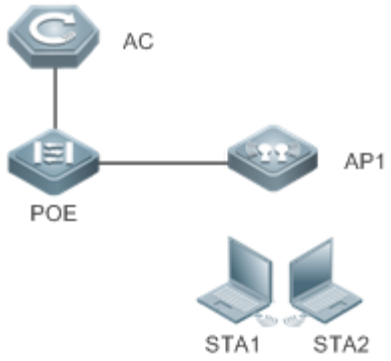
Verification

- Run the show run command to display configuration information.

Configuration Example

Enabling the Broadcast Wireless Forwarding Function

Figure 7-3



Configuration Steps	Enable the broadcast wireless forwarding function in global configuration mode.
AC/AP	`Ruijie#configure terminal` `Ruijie(config)#data-plane wireless-broadcast enable`
Verification	Run the **show running-config** command to display the configuration.
AC/AP	`Ruijie# show ap-config running` `!` `cwmp` `!` `data-plane wireless-broadcast enable` `!`

Common Errors

- N/A

7.5 Monitoring

- N/A

8 Configuring WLOG

8.1 Overview

WLOG (WLAN Log) enables storing and viewing wireless network and STA status in a past period of time. By collecting and storing the information of wireless network, AP and STA in the past 24 hours and then displaying the information through CLI commands, WLOG allows users to analyze the wireless network status and troubleshoot problems.

WLOG is for collecting and storage information, but does not support automatic information analysis temporarily. The WLOG feature is dedicated to enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours to analyze and troubleshoot problems.

Protocols and Standards

- N/A

8.2 Applications

Application	Description
Fit AP Networking	The fit AP networking includes at least one AC and one AP.

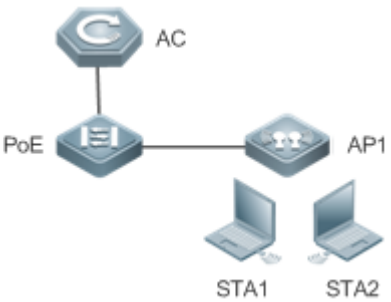
8.2.1 Fit AP Networking

Scenario

Deploy an AC device in a wireless network to query the information on the whole network, AP and STA associated with the AC device.

Figure 8-1 shows the networking topology for viewing the information on the whole network, AP and STA associated with the AC device.

Figure 8-1



Note:	AC: wireless controller PoE: switch, acted as the gateway of the AP

	AP: wireless access device STA1 and STA2: user devices, used as STA

Deployment

- Enable the WLOG feature on an AC device.

8.3 Features

Basic Concepts

Two Modes of Information Collection on the AC

- Periodic Collection

The general information of the whole network, AP and STA is collected and stored on a regular basis (once/1 hour). The general AP and STA information covers all the information of online APs and STAs.

- Reception Advertisement Collection

When an AP behavior of "AP Behavior Type" occurs, the WLOG module is informed to collect and store the information of the behavior.

When a STA behavior of "STA Behavior Type" occurs, the WLOG module is informed to collect and store the information of the behavior.

The information collection on the AP covers only periodic collection of spatial information on all online STAs.

General Information on the Whole Network

- Continuous operation time of the AC
- Number of online APs
- Number of preset but offline APs
- Versions of online APs (number of APs of each version)
- The information on each WLAN (SSID) STA includes:
- Number of online STAs which have passed Web authentication
- Number of online STAs which have passed 802.1x authentication
- Number of online STAs which are authentication-free

General Information on the AP

- AP name
- AP MAC address
- AP IP address
- AP uptime

- Status of each wired port of the AP
- Input/output rate (bits/sec) in last 5 minutes
- Statistics of input/output of unicast, broadcast, multicast and error frames
- General information on each radio
- Working channel
- Transmit power (dBm, absolute value)
- Number of associated online STAs
- Number of online STAs which have passed Web authentication
- Number of online STAs which have passed 802.1x authentication
- Intensity of the co-channel interference signal
- Number of received error frames
- Packet retransmission times

General Information on the STA

- IP address
- Signal strength
- Access rate
- Associated AP, radio and SSID

STA's Spatial Information

- The STA's spatial information mainly includes the statistics of data frame and management frame of the STA, as well as the statistics of each type of rate, as detailed below:
- Number of data frames successfully transmitted (from the AP to the STA)/total traffic
- Number of unresponsive data frames/total traffic
- Number of management frames/total traffic
- Statistics of each type of frames with access rate (The access rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
Access Type (Mbps)	1/2	5.5/11	6/9	12/18	24/36	48/54	Reserved	Reserved

- Statistics of each type of frame with MIMO rate (The MIMO rate is divided into 8 grades for statistics)

Grade	0	1	2	3	4	5	6	7
MIMO Type	mcs0 mcs1	mcs2 mcs3	mcs4 mcs5	mcs6 mcs7	mcs8 mcs9	mcs10 mcs11	mcs12 mcs13	mcs14 mcs15

The spatial information is mainly used to check whether the STA is in low-speed state, whether the proportion of the case in which no ACK frame is transmitted is too high, and whether too many management frames are transmitted and received, so as to further analyze and locate the network problems caused by low speed node, management frame attack, and poor

condition. The STA's spatial information varies in real time, and the current collection frequency is once every five minutes. The information is saved only on the AP due to large data volume.

AP Behavior Type

The AP behavior type includes going online, going offline and CAPWAP connection failure.

STA Behavior Type

The STA behavior type includes: association, de-association, Web authentication going online, Web authentication offline, 802.1X authentication going online, and 802.1X authentication offline.

Features

Feature	Description
Enabling the WLOG Feature	You can enable the WLOG feature to automatically collect AC, AP and STA information.
Synchronizing STA Go-online/offline Information to the ELOG Server	Synchronize STA go-online/offline information to the ELOG server.
Configuring the AP Detective Function	An AP detects information about STAs and hotspots nearby.
Synchronizing Information Detected by an AP to the ELOG Server	An AC synchronizes STA information and hotspot information detected by an AP to the ELOG server.

8.3.1 Enabling the WLOG Feature

After the WLOG feature is enabled, the AC or AP automatically collects AC, AP and STA information and records the information into memory, enabling users, with provided information, to have a more accurate understanding of the wireless network and STA status in the past 24 hours and analyze and troubleshoot problems.

Working Principle

After the WLOG feature is enabled, the AC or AP automatically collects AC, AP and STA information and records the information into memory, and receives online/offline advertisement of the AP and STA and records into memory for users to view.

8.3.2 Synchronizing STA Go-online/offline Information to the ELOG Server

After the WLOG function is enabled and the ELOG server URL is configured, the AC sends STA information to the ELOG server when a STA goes online or offline.

Working Principle

After the WLOG function is enabled and the AC receives the STA go-online/offline notice, the AC sends STA information in a specific format to the ELOG server.

8.3.3 Configuring the AP Detective Function

The AP detective function is used to detect STAs and hotspots around an AP. The AP detective function can be configured to detect either or both of STAs and hotspots.

Working Principle

After an AC delivers the command of enabling the AP detective function, the AP periodically reports the detected information to the AC for reprocessing.

8.3.4 Synchronizing Information Detected by an AP to the ELOG Server

An AC reports information detected by an AP to the ELOG server.

Working Principle

An AC reports information detected by an AP in a specific format to the ELOG server.

8.4 Configuration

Configuration	Description and Command	
Enabling the WLOG Feature	⚠ (Mandatory) It is used to enable the WLOG feature.	
	wlan diag enable	Enables the WLOG feature
Synchronizing STA Go-online/offline Information to the ELOG Server	⚠ (Optional) It is used to synchronize STA go-online/offline information to the ELOG server.	
	web-server enable api-path assoc-sta url url	Configures the address of the ELOG server.
Configuring the AP Detective Function	(Optional) It is used to enable the detective function of an AP.	
	ap-probe ap enable	Enables the hotspot information detective function of an AP.
	ap-probe sta enable	Enables the STA information detective function of an AP.
	ap-probe cache-time	Configures the time for caching detected information (aging) for an AP.
	ap-probe upload-time	Configures the interval for periodically reporting detected information for an AP.
	ap-probe limit	Configures the number of non-repetitive detected information records that can be received within aging period for the AP.

Synchronizing Information Detected by an AP to the ELOG Server	(Optional) It is used to synchronize information detected by an AP to the ELOG function.	
	web-server enable api-path probe-ap url *url*	Configures the ELOG address to which the hotspot information detected by an AP is synchronized.
	web-server enable api-path probe-sta url *url*	Configures the ELOG address to which the STA information detected by an AP is synchronized.

8.4.1 Enabling the WLOG Feature

Configuration Effect

- After the WLOG feature is enabled, the AC or AP automatically records the AC, AP and STA information.

Notes

- Enabling the WLOG feature pre-allocates memory. If the memory is not sufficient, the WLOG feature cannot be enabled. Disabling the WLOG feature frees all memory for information storage and pre-allocated memory.

Configuration Steps

↘ Enabling the WLOG Feature

- (Mandatory) Run the **wlog diag enable** command to enable the WLOG feature.
- Enable the WLOG feature in global configuration mode of the AC device.
- After the WLOG feature is enabled, information is collected and recorded into memory on a regular basis.

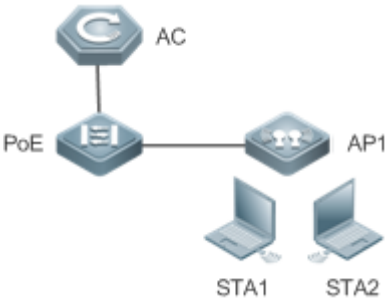
Command	**wlan diag enable**
Parameter Description	N/A
Defaults	By default, the WLOG feature is disabled on the AC and AP device.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show wlan diag network** command to check whether the whole network information can be viewed on the AC.
- Run the **show wlan diag sta** command to check whether the STA information can be viewed on the AP.

Configuration Example

↘ Enabling the WLOG Feature

Scenario **Figure 8-2**	
Configuration Steps	● Enable the WLOG feature in global configuration mode.
AC	`Ruijie# configure terminal` `Ruijie(config)# wlan diag enable`
Verification	Use the **show wlan diag network** command to display the general information of the whole network.
AC	`Ruijie# show wlan diag network` `Time: 2017-05-05 14:57:07` `AC uptime: 10 h` `Online AP: 1` `Offline AP:0` `Online AP Version:` `PID HwVer SwVer AP Number` `--- --- ---` `AP520 1.00 AP_RGOS 11.1(5)B9P2, Release(04162423) 1` `Wlan information:` `WLAN ID SSID Active STA WEB Auth 1X Auth Other` `--- --- --- --- --- ---` `4 wlan-guest 2 2 0 0` `5 wlan-802.1x 6 0 6 0`

8.4.2 Synchronizing STA Go-online/offline Information to the ELOG Server

Configuration Effect

- After the WLOG function is enabled and the ELOG server URL is configured, the AC sends the STA go-online/offline information to the ELOG server.

Notes

- This function is triggered by the STA go-online/offline action. Before the function is enabled, the STA go-online/offline information is not sent to the ELOG server.

Configuration Steps

↘ Configuring the URL of the ELOG Server

- The complete address of the ELOG server needs to be configured.

Command	**web-server enable api-path assoc-sta url** *url*
Parameter Description	*url*: indicates the complete address of the ELOG server.
Defaults	By default, The ELOG server URL is not configured, that is, the AC does not interwork with the ELOG server.
Command Mode	Global configuration mode
Usage Guide	To ensure smooth data transmission, the WLOG function needs to be enabled. In local forwarding scenarios, if the AC does not obtain the STA IP address (which can be queried by running the **show ac-config client** command) after the STA goes online, run the **ip dhcp snooping** command in global configuration mode to ensure that the AC can obtain the STA IP address. Up to eight Elog servers are supported.

Verification

- Run the **show running** command to display configurations.

Configuration Example

↘ Configuring the URL of the ELOG Server

Configuration Steps	● In global configuration mode, configure two Elog server URLs.
AC	`Ruijie# configure terminal` `Ruijie(config)#web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta` `Ruijie(config)# web-server enable api-path assoc-sta url http://172.18.155.15:8080/elog/service/dc/updateSta`
Verification	Run the **show running-config** command to display configurations.

AC	Ruijie# show running-config ! web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta http://172.18.155.14:8080/elog/service/dc/updateSta web-server enable api-path assoc-sta url http://172.18.155.15:8080/elog/service/dc/updateSta !

Common Errors

- Only an IP address instead of a complete URL is specified in the URL parameter.

Common Errors

- N/A

8.4.3 Configure the AP Detective Function

Configuration Effect

After an AC delivers the command of enabling the AP detective function, the AP periodically reports detected STA information and hotspot information to the AC.

Configuration Steps

Enabling the Hotspot Information Detective Function of an AP

- Optional. After the function is enabled, an AP can detect hotspot information.

Command	**ap-probe ap enable**
Parameter Description	*N/A*
Defaults	This function is not configured by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	N/A

Enabling the STA Information Detective Function of an AP

- Optional. After the function is enabled, an AP can detect STA information.

Command	**ap-probe sta enable**
Parameter Description	*N/A*
Defaults	This function is not configured by default.

Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring the Time for Caching Detected Information (Aging) for an AP

- Optional. Configure the time for caching detected information by an AP on the AP.

Command	**ap-probe cache-time** *time*
Parameter Description	*time*: Indicates the cache time(aging time). The value ranges from 0 to 3600 seconds.
Defaults	The default value is 120 seconds.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	When the time is set to **0**, detected information is not cached on the AP. As a result, considerable repeated information is reported to the AC, and the CPU usage is very high due to frequent transmission of packets, which affects the wireless service. Therefore, it is set to **0** during commissioning and it is not recommended to **0** in normal cases.

Configuring the Interval for Periodically Reporting Detected Information for an AP

- Optional. Configure the interval for periodically reporting detected information for an AP.

Command	**ap-probe upload-time** *time*
Parameter Description	*time*: Indicates the interval for periodically reporting detected information. The value ranges from 1 to 300 seconds.
Defaults	The default value is 5 seconds.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Detected Information Records That Can Be Cached on an AP

- Optional. Configure the number of non-repetitive detected information records that can be received within the aging period for the AP.

Command	**ap-probe limit** *num*
Parameter Description	*num*: Indicates the number of detected information records that can be cached on an AP. The value ranges from 1 to 65535 and the maximum value depends on the number of detected information records supported by the AP.
Defaults	The default value is 100.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	If the configured value of *num* exceeds the maximum number of information records supported by an AP, the maximum number of information records supported by the AP prevails. Cached information occupies certain memory resources. Therefore, it is not recommended to set it to a large number.

Verification

- Run the **show running** command to display the configuration in AP group configuration mode and all-AP configuration mode.
- Run the **show ap-config running** command to display the configuration in AP configuration mode.

Configuration Example

↘ Enabling the Snooping Function of AP 1

Configuration Steps	● Enable the hotspot and STA detective function in AP configuration mode. Set the cache time to 60 seconds, report interval to 6 seconds, and the number of non-repetitive detected information that can be cached to 200.
AC	`Ruijie# configure terminal` `Ruijie(config)#ap-config AP1` `You are going to config AP(AP1), which is online now.` `Ruijie(config-ap)#ap-probe ap enable` `Ruijie(config-ap)#ap-probe sta enable` `Ruijie(config-ap)#ap-probe cache-time 60` `Ruijie(config-ap)#ap-probe upload-time 6` `Ruijie(config-ap)#ap-probe limit 200` `Ruijie(config-ap)#`
Verification	Run the **show ap-config running** command to display the configuration.
AC	`Ruijie# show ap-config running` `!` `ap-config AP1` ` ap-mac 1234.1234.5656` ` ap-probe sta enable` ` ap-probe ap enable` ` ap-probe upload-time 6` ` ap-probe cache-time 60` ` ap-probe limit 200` `!`

8.4.4 Synchronizing Information Detected by an AP to the ELOG Server

Configuration Effect

- After the hotspot information detective function of an AP is enabled and the URL of the ELOG server, to which the detected hotspot information is synchronized, is configured, the AC sends the snooped hotspot information reported by the AP to the ELOG server.
- After the STA information detective function of an AP is enabled and the URL of the ELOG server, to which the detected

STA information is synchronized, is configured, the AC sends the detected STA information reported by the AP to the ELOG server.

Configuration Steps

Configuring the URL of the ELOG Server to Which Hotspot Information Detected by an AP Is Synchronized

- The complete address of the ELOG server needs to be configured.

Command	**web-server enable api-path probe-ap url** *url*
Parameter Description	*url*: Indicates the complete address of the ELOG server for storing detected hotspot information.
Defaults	By default, The ELOG server URL is not configured, that is, an AC is not interconnected to the ELOG server.
Command Mode	Global configuration mode
Usage Guide	A maximum of eight ELOG servers can be configured.

Configuring the URL of the ELOG Server to Which STA Information Snooped by an AP Is Synchronized

- The complete address of the ELOG server needs to be configured.

Command	**web-server enable api-path probe-sta url** *url*
Parameter Description	*url*: Indicates the complete address of the ELOG server for storing detected STA information.
Defaults	By default, The ELOG server URL is not configured, that is, an AC is not interconnected to the ELOG server.
Command Mode	Global configuration mode
Usage Guide	A maximum of eight ELOG servers can be configured.

Verification

Run the **show running** command to display configurations.

Configuration Example

Configuring the URL of the ELOG Server to Which Information Snooped by an AP Is Synchronized

Configuration Steps	• In global configuration mode, set the URL of the first ELOG server for storing detected hotspot information to http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid and the URL of the second ELOG server to http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid. • In global configuration mode, set the URL of the first ELOG server for storing detected STA information to http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta and the URL of the second ELOG server to http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta.
AC	`Ruijie# configure terminal` `Ruijie(config)# web-server enable api-path probe-ap url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid` `Ruijie(config)# web-server enable api-path probe-ap url`

	http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid Ruijie(config)# web-server enable api-path probe-sta url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta Ruijie(config)# web-server enable api-path probe-sta url http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta
Verification	Run the **show running-config** command to display configurations.
AC	Ruijie# show running-config ! web-server enable api-path probe-ap url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid web-server enable api-path probe-sta url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta!

8.5 Monitoring

Displaying

Description	Command
Displays the general information on the whole network	**show wlan diag network**
Displays the AP information on the AC	**show wlan diag ap** [**ap-mac** *ap-mac*] [**number** *number*]
Displays the STA information on the AC	**show wlan diag sta** [**sta-mac** *sta-mac*] [**ip-range** *ip-prefix*] [**action** *action* [**result** *result*]] [**number** *number*]

9 Configuring Roaming

9.1 Overview

Roaming is a function that allows re-association of stations (STAs) with access points (APs) when STAs move in the coverage areas of different APs.

The roaming function enables moving STAs to maintain the ongoing IP communication and enjoy all applications and services. Roaming is transparent and seamless for users without data interruption.

If STAs move in different areas in a wireless environment, the roaming function must be supported. Roaming scenarios are classified into two types: intra-AC roaming and inter-AC roaming.

- Intra-AC roaming is applicable for deployments having only one access controller (AC).
- Inter-AC roaming is applicable for deployments having multiple ACs.

Protocols and Standards

- N/A

9.2 Applications

Application	Description
Intra-AC Roaming	One STA is associated with AP1 joined to one AC, and then moves to the coverage of AP2 joined to the same AC and is associated with AP2.
Inter-AC Roaming	One STA is associated with AP1 joined to AC1, and then moves to the coverage of AP2 joined to AC2 and is associated with AP2.

9.2.1 Intra-AC Roaming

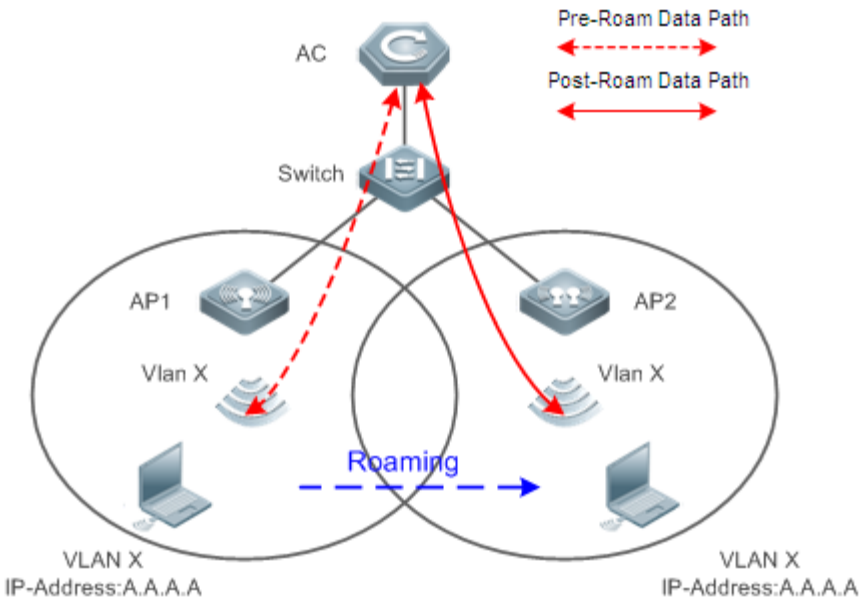
Scenario

One STA is associated with AP1 joined to one AC, and then moves to the coverage of AP2 joined to the same AC and is associated with AP2.Based on the entity (AC or AP) that forwards data, intra-AC roaming is further classified into intra-AC L2/L3 roaming in centralized forwarding mode and intra-AC L2/L3 roaming in local forwarding mode.

9.2.1.1 Intra-AC L2/L3 Roaming in Centralized Forwarding Mode

Figure 9-1 shows intra-AC L2/L3 roaming in centralized forwarding mode.

Figure 9-1 Intra-AC L2/L3 Roaming in Centralized Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with the STA. (If the VLAN X corresponding to AP2 is changed to VLAN Y, L3 roaming occurs.)

Unlike L2 roaming, VLANs associated with the STA are different before and after roaming. Except this difference, other processing is the same in L2 and L3 roaming. Therefore, L2 roaming and L3 roaming are not discussed separately hereinafter.

Deployment

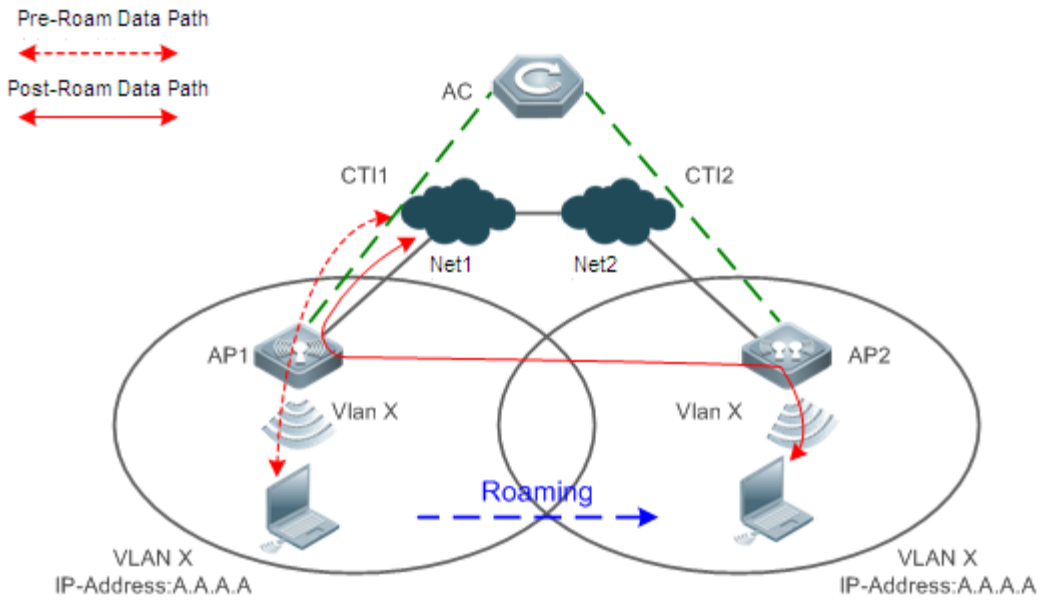
- AP1 and AP2 are associated with the AC through switches and are assigned to the same WLAN.
- At first, the STA is associated with AP1, and the obtained IP address is A.A.A.A.
- Later, the STA moves to the coverage of AP2, and is associated with AP2. The IP address remains unchanged without communication interruption.

STA roaming is implemented only when the wireless service set identifiers (SSIDs) provided by AP1 and AP2 are the same.

9.2.1.2 Intra-AC L2/L3 Roaming in Local Forwarding Mode

Figures 9-2 shows intra-AC L2/L3 roaming in local forwarding mode.

Figure 9-2 Intra-AC L2/L3 Roaming in Local Forwarding Mode



Remarks	CTI is the communication tunnel between an AP and an AC. VLAN X indicates the VLAN ID associated with the STA.

Deployment

- AP1 and AP2 set up a control channel with the AC through the CTI, and are assigned with the same WLAN. The corresponding VLAN is VLAN X.
- AP1 and AP2 work in local forwarding mode. At first, the STA is associated with AP1, and the obtained IP address is A.A.A.A.
- Later, the STA moves to the coverage of AP2, and is associated with AP2. The IP address remains unchanged without communication interruption.
- Before roaming, the data is directly sent out by AP1. After roaming, the data is forwarded from AP2 to AP1, and then sent out by AP1.

STA roaming is implemented only when the wireless SSIDs provided by AP1 and AP2 are the same.

9.2.2 Inter-AC Roaming

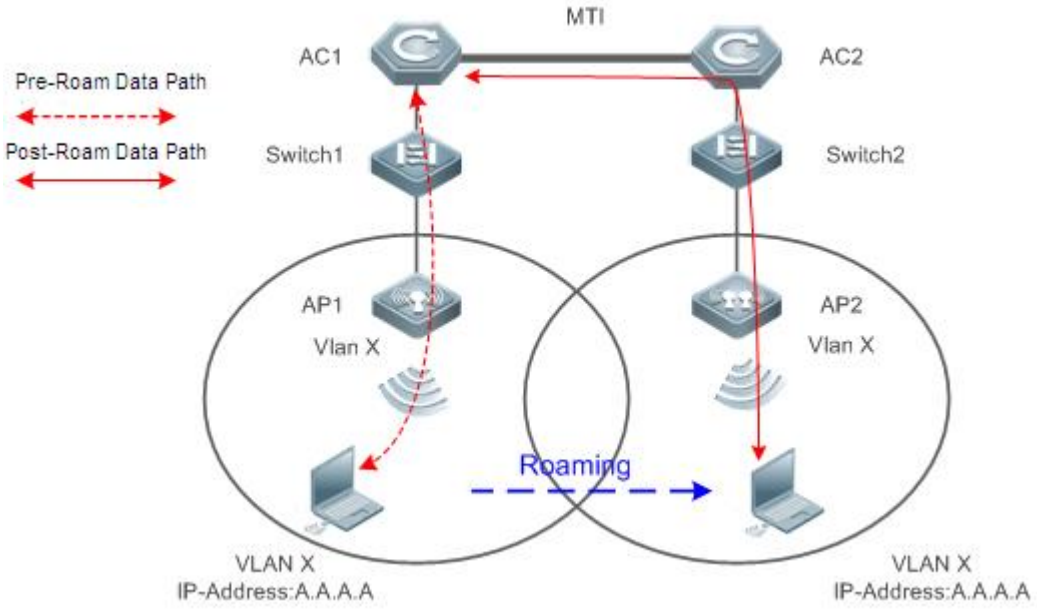
Scenario

One STA is associated with AP1 joined to AC1, and then moves to the coverage of AP2 joined to AC2 and is associated with AP2.Based on the entity (AC or AP) that forwards data, inter-AC roaming is further classified into inter-AC roaming in centralized forwarding mode and inter-AC roaming in local forwarding mode.

9.2.2.1 Inter-AC L2/L3 Roaming in Centralized Forwarding Mode

Figure 9-3 shows inter-AC L2/L3 roaming in centralized forwarding mode.

Figure 9-3 Inter-AC L2/L3 Roaming in Centralized Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with the STA. MTI is the communication tunnel between ACs.

Deployment

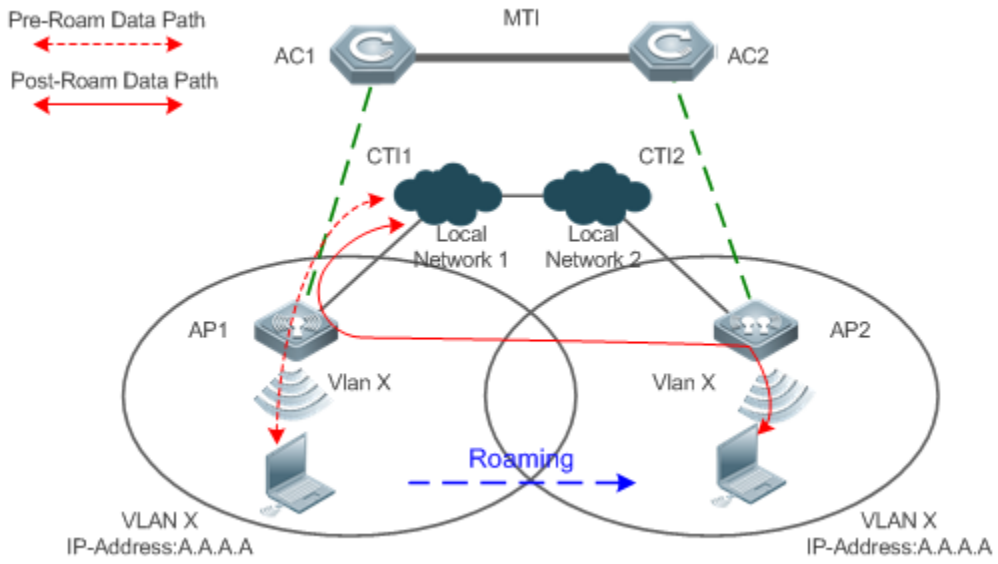
- AC1 and AC2 are configured as the mobility member of the peer AC, and can communicate with each other.
- AP1 is connected to AC1, and AP2 is connected to AC2. Both AP1 and AP2 are assigned to the same WALN. The corresponding VLAN is VLAN X.
- At first, the STA is associated with AP1, and the obtained IP address is A.A.A.A. Later, the STA moves to the coverage of AP2, and is associated with AP2. The IP address remains unchanged without communication interruption.
- Before roaming, the data is directly sent out by AC1. After roaming, the data is forwarded from AC2 to AC1 through the MTI, and then sent out by AC1.

⚠ STA roaming is implemented only when the wireless SSIDs provided by AP1 and AP2 are the same.

9.2.2.2 Inter-AC L2/L3 Roaming in Local Forwarding Mode

Figure 9-4 shows inter-AC L2/L3 roaming in local forwarding mode.

Figure 9-4 Inter-AC L2/L3 Roaming in Local Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with the STA. MTI is the communication tunnel between ACs, and CTI is the communication tunnel between APs and ACs.

Deployment

- AC1 and AC2 are included in the same mobility group, and are configured as the mobility member of the peer AC.
- AP1 is connected to AC1, and AP2 is connected to AC2. Both AP1 and AP2 are assigned to the same WALN. The corresponding VLAN is VLAN X. Both AP1 and AP2 work in local forwarding mode.
- At first, the STA is associated with AP1, and the obtained IP address is A.A.A.A. Later, the STA moves to the coverage of AP2, and is associated with AP2. The IP address remains unchanged without communication interruption.
- Before roaming, the data is directly sent out by AP1. After roaming, the data is forwarded from AP2 to AP1, and then sent out by AP1.

⚠ STA roaming is implemented only when the wireless SSIDs provided by AP1 and AP2 are the same.

9.3 Features

Basic Concepts

Association and Re-Association

Association: A STA selects an extended service area, and sends the asso frame to set up a connection with this extended service area.

Re-association: A STA moves from a basic service area of an extended service area to another basic service area of this extended service area, and is associated with a new AP. In this case, the STA sends the reasso frame.

STA, AP, and AC

STA: It is a wireless workstation that is equipped with the wireless network interface card (NIC), such as a laptop computer or a mobile phone.

AP:It is a wireless access point that provides radio signals so that the STA can access the wireless network.

AC: It is a wireless access controller that provides wireless connection and related service functions.

L2 Roaming and L3 Roaming

L2 roaming: The VLAN to which a STA belongs remains unchanged before and after roaming.

L3 roaming: The VLAN to which a STA belongs changes after roaming.

Centralized Forwarding and Local Forwarding

Centralized forwarding: All packets of a STA are forwarded by the AC.

Local forwarding: Control packets of a STA are processed by the AC, whereas data packets are directly forwarded by the AP.

Intra-AC Roaming and Inter-AC Roaming

Intra-AC roaming:A STA roams from one AP joined to an AC to another AP joined to the same AC.

Inter-AC roaming:A STA roams from an AP joined to an AC to another AP joined to a different AC.

Home AC and Foreign AC

- Home AC (HA): When a STA is associated with an AC in the mobility group for the first time, this AC is called HA of the STA.
- Foreign AC (FA): A STA is currently connected to an AC that is not the HA. This AC is called FA of the STA.

For the intra-AC roaming, the HA is the same as the FA.

Overview

Feature	Description
Mobility Group	After a mobility group is configured, a STA can roam to different ACs in the same mobility group.

Mobility List	The mobility list is an extension of the mobility group. The number of AC members in the mobility group is limited. The mobilizing list is introduced to extend the roaming scope of STAs without affecting roaming of the mobility group.
Displaying STA Roaming Status and Roaming Tracks	Displays the current status of all roaming STAs on the local AC and the roaming track of a STA.
Suppressing STA Roaming Syslogs	Suppresses the output rate of STA roaming syslogs.

9.3.1 Mobility Group

The roaming scope of wireless STAs within a WLAN cannot be expanded without limit. To enable a STA to roam among APs joined to different ACs and manage the roaming scope of STAs, a mobility group is defined to include a group of ACs within the STA roaming scope.

Working Principle

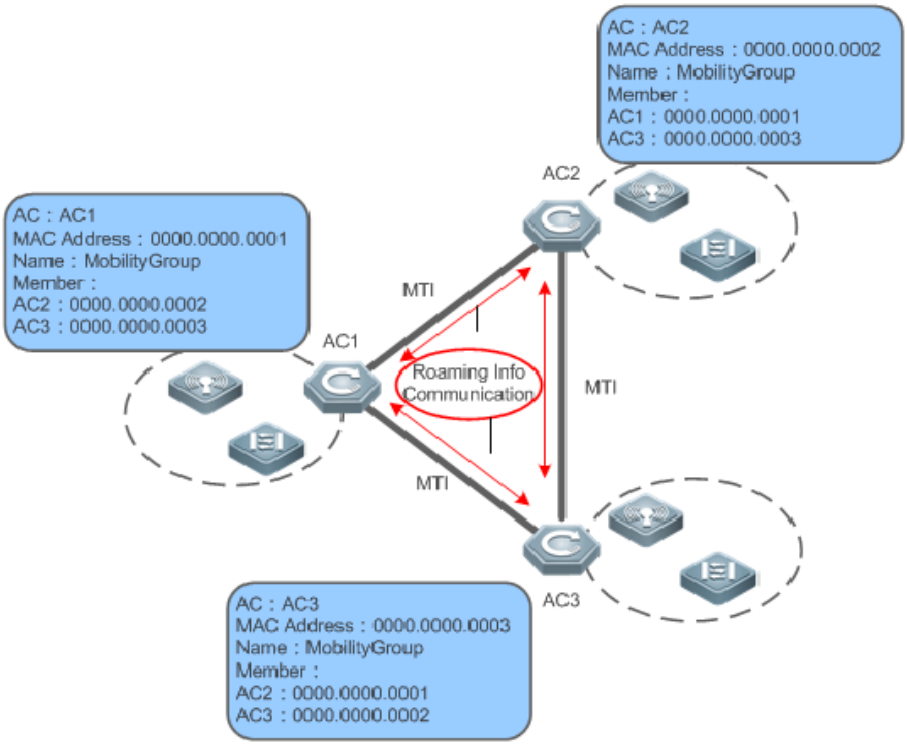
Each AC is configured with a list of other members of the mobility group. When a STA joins an AC, the AC sends out a message to all of the ACs in the mobility group. If it is the first time the STA accesses the mobility group, the initial AC (HA) will save information about the STA. When the STA roams to another AC (FA), the HA synchronizes the STA information to the FA. If this STA is roaming, the HA synchronizes the STA information to the current AC (FA) after receiving a message.

Generally, the roaming STA information is exchanged only after roaming occurs. Before roaming occurs, the information synchronization function of the mobility group can be used to proactively share STA information among ACs in the mobility group. This saves time in STA roaming and improves the roaming efficiency.

↘ Topology of the Mobility Group

ACs in the mobility group encapsulate and transfer roaming information through the Controlling and Provisioning of Wireless Access Point (CAPWAP) tunnel. The unique technology reduces the re-authentication time on the Radius server after inter-AC roaming of STAs, and accelerates information authentication of roaming STAs, laying a solid foundation for seamless roaming. Figure 9-2 shows the topology of the mobility group.

Figure 9-5 Topology of the Mobility Group



Remarks	MTI is the communication tunnel between ACs. AC1, AC2, and AC3 are in the same mobility group. On each AC, another two ACs are configured as its mobility member.

9.3.2 Mobility List

The mobility list is an extension of the mobility group. The number of AC members in the mobility group is limited. The mobility list is introduced to extend the roaming scope of STAs without affecting roaming of the mobility group.

Working Principle

↘ Comparison Between the Mobility List and the Mobility Group

Data exchange of roaming STAs in the mobility list is similar with that in the mobility group. The major difference is as follows: Intra-group roaming adopts Proactive Key Caching (PKC), while inter-group roaming uses the mobility list that requires the roaming STA to complete the entire authentication process with the AAA/Radius server. Therefore, compared with intra-group roaming, inter-group roaming presents a relatively low efficiency. The common thing between the mobility group and the mobility list is that the roaming process is seamless and transparent for users.

A mobility group can be designated for a specific AC. Then, STAs associated with this AC can roam in this mobility group. In addition to configuration of a mobility group, you can also configure a mobility list on the AC. The member ACs in the mobility list must be in a mobility group different from that of the current AC. In this way, STAs on the current AC can roam across mobility groups.

9.3.3 Displaying STA Roaming Status and Roaming Tracks

To learn the roaming status and movements of all STAs on an AC, you can check the status and roaming tracks of current roaming STAs.

Working Principle

Information about roaming STAs is recorded on the HA, including the roaming type, connected WLAN, as well as VLANs, APs, and pre-roaming/post-roaming radios. Such information is stored, and deleted only when the STA is deassociated.

⚠ The roaming track is recorded by default.

⚠ You can run the **show mobility user roam- track** command to display the tracks of roaming STAs.

9.3.4 Suppressing STA Roaming Syslogs

STA roaming syslog suppression prevents a high CPU usage caused by the large amount of syslogs output during roaming of a large number of STAs.

Working Principle

The number of syslog records output per second is counted. When this number reaches the upper limit, no more syslog is output within the second, thereby suppressing the syslogs. In the next second, the number of syslogs is counted again.

9.3.5 Preventing STA Roaming

Roaming prevention is configured to facilitate distribution and use of WLAN resources.

Working Principle

When an AC receives a roaming request, it checks whether the roam-in/roam-out WLAN has been configured with roaming prevention, If yes, the STA is prevented from roaming.

9.4 Configuration

Configuration	Description and Command	
Configuring a Mobility Group	⚠ (Optional) It is used to implement the inter-AC roaming function.	
	mobility-group	Configures a mobility group.
	member	Adds or deletes a mobility member to or from the mobility group.
Configuring Proactive Information Exchange Within the Mobility Group	⚠ (Optional) It is used to exchange STA information within the mobility group.	
	mobility-fast	Enables proactive information exchange within the mobility group.
Configuring a Mobility List	⚠ (Optional) It is used to add members to a mobility list.	

	list	Adds or deletes member ACs to or from the mobility list.
Configuring the Maximum Number of Times a Keepalive Packet Can Be Transmitted	(Optional) It is used to configure the maximum number of times a keepalive packet can be transmitted. If this number is exceeded, the keepalive attempt fails.	
	keepalive-count	Configures the maximum number of times a keepalive packet can be transmitted
Configuring the Interval at Which a Keepalive Packet Is Sent	(Optional) It is used to configure the interval at which a keepalive packet is sent.	
	keepalive-interval	Configures the interval at which a keepalive packet is sent.
Testing Roaming Connectivity	(Optional) It is used to test whether ACs in the mobility are interconnected properly.	
	mti-ping	Tests the connectivity of tunnels between ACs in the mobility group.
Suppressing STA Roaming Syslogs	(Optional) It is used to suppress the output rate of STA roaming syslogs.	
	roaming logging rate-limit	Sets the output rate of STA roaming syslogs.
Preventing STA Roaming	(Optional) It is used to prevent STA roaming.	
	no roaming support wlan	Prevents STA roaming.

9.4.1 Configuring a Mobility Group

Configuration Effect

- Configure a mobility group and add a mobility member to implement inter-AC roaming.
- The centralized forwarding mode is configured in the same way as the local forwarding mode.

Notes

- The precondition of inter-AC roaming is that the two ACs can communicate with each other normally.

Configuration Steps

Creating a Mobility Group

- (Optional) The configuration is mandatory if inter-AC roaming should be implemented. Run the **mobility-group** *group-name* command to create a mobility group.
- Configure at least one mobility group on every AC that involves inter-AC roaming.

Up to eight mobility groups can be created on an AC.

Command	**mobility-group** *group-name*

Parameter Description	*group-name*: Specifies the name of a mobility group.
Defaults	No mobility group is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding Mobility Members

- (Optional) The configuration is mandatory if inter-AC roaming should be implemented.
- Add at least one member to a mobility group on every AC that involves inter-AC roaming.
- After a mobility group is created, there is no mobility member in the group. Therefore, you need to add one or more mobility members.
- To ensure efficiency and reliability of information synchronization between ACs within a mobility group, you must limit the number of members in the mobility group. A mobility group supports up to 24 AC members.

Command	**member** {*ip-address*|*ipv6-address*}
Parameter Description	*ip-address:* Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of an mobility member.
Defaults	A newly created mobility group does not contain any member.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

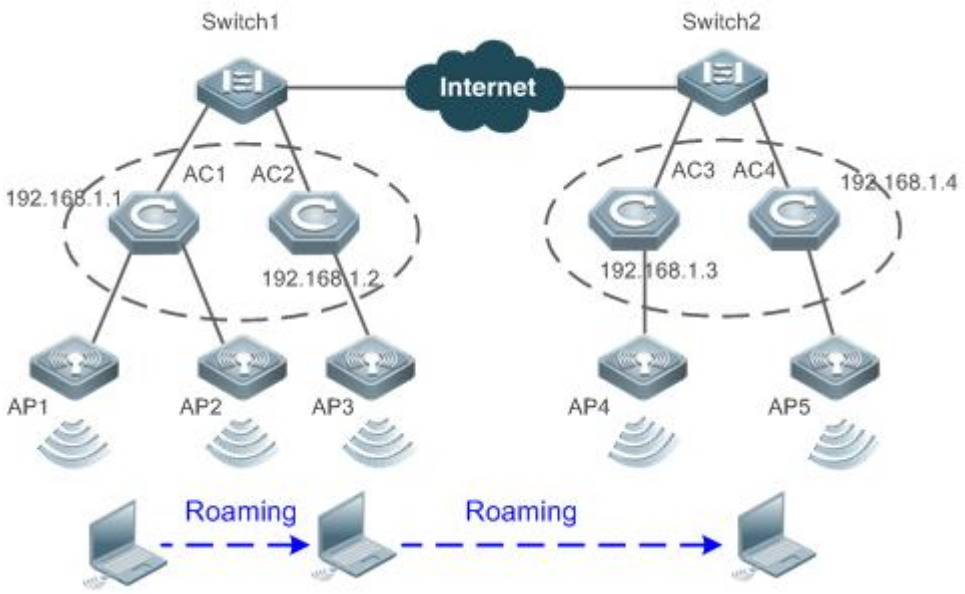
Verification

Check the mobility group information to determine whether members are successfully added and whether the connections are normal.

Configuration Example

All the configuration examples in this document are provided for the scenario of inter-AC roaming in centralized forwarding mode.

Configuring a Mobility Group and Adding a Member to this Group

Scenario **Figure 9-6**	 ● Inter-AC or intra-AC Roaming Scenario
Configuration Steps	● Set the loopback address of AC1 to 192.168.1.1 and the loopback address of AC2 to 192.168.1.2, and ensure that one AC can be pinged successfully from another AC. ● Add a mobility group. ● Add a mobility member.
AC1	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#mobility-groupmgroup_name Ruijie(config-mobility)#member 192.168.1.1
AC2	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#mobility-groupmgroup_name Ruijie(config-mobility)#member 192.168.1.2
Verification	Check the mobility group information to determine the configurations are successful. ● Run the **show mobility status** *mgroup_name* command on every AC.

AC1	Ruijie# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... normal Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.1Client OK OK Mobility List Members:
AC2	Ruijie# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... normal Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.2Client OK OK Mobility List Members:

Common Errors

- Mobility AC members fail to ping each other.
- The mobility group or members are not configured on an AC.
- The mobility group names are inconsistent.

9.4.2 Configuring Proactive Information Exchange within the Mobility Group

Configuration Effect

- When roaming does not occur, an AC also shares the STA information with other AC members in the mobility group.

Notes

- A mobility group must be configured.

Configuration Steps

- (Optional) After configuring a mobility group on ACs, enter mobility group configuration mode and enable proactive information exchange.
- (Optional) Configure fast roaming as required.

Command	mobility-fast
Parameter Description	N/A
Defaults	Proactive information exchange is disabled by default.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

- Check the mobility group information. If the mobility group status is Fast Mode, the configuration is successful.

Configuration Example

Configuring Proactive Information Exchange within the Mobility Group

Configuration Steps	• Configure a mobility group.(The configurations are omitted here.) • Enable proactive information exchange within the mobility group.
AC	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#mobility-groupmgroup_name Ruijie(config-mobility)# mobility-fast
Verification	Check the mobility group information.
AC	Ruijie# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... Fast Mode .....

Common Errors

- N/A

9.4.3 Configuring a Mobility List

Configuration Effect

- When no more members can be added to the mobility groups, apply the mobility list to implement roaming.

Notes

- A mobility group must be configured.

Configuration Steps

- (Optional) Add members to the mobility list after a mobility group is configured on the AC. Run the **list** { *ip-address* | *ipv6-address* } command to add a member to the mobility list.
- If the number of mobility members exceeds the capacity of the mobility group, you can add members to the mobility list as an alternative.

A mobility list supports up to 72 members.

Command	**list** {*ip-address*| *ipv6-address*}
Parameter Description	*ip-address*: Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of a mobility member.
Defaults	No mobility list is configured by default.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

- Check the mobility group information to determine whether added members exist.

Configuration Example

Configuring a Mobility List

Configuration Steps	● Configure a mobility group. (The configurations are omitted here.) ● Add members to the mobility list.
AC	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#mobility-groupmgroup_name Ruijie(config-mobility)# list 192.168.1.1 Ruijie(config-mobility)# list 192.168.1.2

Verification	Check the mobility list information.
AC	Ruijie# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... Fast Mode Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel Mobility List Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.2 Client OK OK 192.168.1.1 Client OK OK

Common Errors

- N/A

9.4.4 Configuring the Maximum Number of Times a Keepalive Packet Can Be Transmitted

Configuration Effect

- (Optional) Configure the maximum number of times a keepalive packet can be transmitted. If this number is exceeded, the keepalive attempt fails.

Notes

- A mobility group must be configured and have at least one mobility member.

Configuration Steps

- (Optional) Configure a mobility group on the AC, and enter mobility group configuration mode.
- The maximum number of times a keepalive packet can be transmitted is not modified by default. If the network environment is unstable, you can increase this value.

Command	**keepalive-count** *counts*
Parameter Description	*counts*: Indicates the keepalive times. The value ranges from 2 to 30.

Defaults	4 times after a mobility group is created
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

- Check the mobility group information. The maximum number of times a keepalive packet can be transmitted should be displayed.

Configuration Example

↘ Configuring the Maximum Number of Times a Keepalive Packet Can Be Transmitted

Configuration Steps	● Configure a mobility group. (The configurations are omitted here.) ● Set the maximum number of times a keepalive packet can be transmitted to 5.
AC	`Ruijie(config)#mobility-group mgroup_name` `Ruijie(config-mobility)# keepalive-count 5`
Verification	Check the mobility group configurations.
AC	`Ruijie# show mobility status mgroup_name` `Mobility Group mgroup_name` `Mobility Keepalive Interval..... 10` `Mobility Keepalive Count..... 5` `Mobility Group Status..... normal`

Common Errors

- N/A

9.4.5 Configuring the Interval at Which a Keepalive Packet Is Sent

Configuration Effect

- (Optional) Configure the interval at which a keepalive packet is sent.

Notes

- A mobility group must be configured and have at least one mobility member.

Configuration Steps

- (Optional) Configure a mobility group on the AC, and enter mobility group configuration mode.

- The interval at which a keepalive packet is sent is 10s by default. If the network environment is unstable, you can increase the interval.

Command	**keepalive- interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which a keepalive packet is sent. The unit is second. The value ranges from 1 to 30.
Defaults	10s after a mobility group is created
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

- Check the mobility group information. The interval at which a keepalive packet is sent should be displayed.

Configuration Example

Configuring the Interval at Which a Keepalive Packet Is Sent

Configuration Steps	• Configure a mobility group. (The configurations are omitted here.) • Set the interval at which a keepalive packet is sent to 20s.
AC	`Ruijie(config)#mobility-group mgroup_name` `Ruijie(config-mobility)# keepalive-interval20`
Verification	Check the mobility group configurations.
AC	`Ruijie# show mobility status mgroup_name` `Mobility Group mgroup_name` `Mobility Keepalive Interval..... 20` `Mobility Keepalive Count..... 4` `Mobility Group Status..... normal`

Common Errors

- N/A

9.4.6 Testing Roaming Connectivity

Configuration Effect

- (Optional) Start a connectivity test to check whether member ACs are connected with each other normally.

Notes

- A mobility group must be configured and have at least one mobility member.

Configuration Steps

- (Optional) After configuring a mobility group on the AC, enter mobility group configuration mode to start a connectivity test.
- Start a connectivity test to check whether member ACs in the mobility group communicate with each other normally,.

Command	**mti-ping** {*ip-address*|*ipv6-address*}
Parameter Description	*ip-address*: Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of a mobility member.
Defaults	N/A
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

- Check the test results.

Configuration Example

Starting a Roaming Connectivity Test

Configuration Steps	• Configure a mobility group and add mobility members. (The configurations are omitted here.) • Start a roaming connectivity test.
AC	`Ruijie(config)#mobility-group my_group_name` `Ruijie(config-mobility)#mti-ping 192.168.1.2` `Sending 4, MTI packet to 192.168.1.1, timeout is 2 seconds:` `!!!!` `Success rate is 100 percent (4/4)`
Verification	Check the test results.
AC	`Sending 4, MTI packet to 192.168.1.1, timeout is 2 seconds:` `!!!!` `Success rate is 100 percent (4/4)`

Common Errors

- The **mti-ping** command is different from the **ping** command, that is, successful execution of the **ping** command does not mean that execution of the **mti-ping** command is also successful. The **mti-ping** command is applicable to mobility group members.

9.4.7 Suppressing STA Roaming Syslogs

Configuration Effect

- Even if STAs roam frequently, the number of roaming syslogs output per second does not exceed the limit.

Notes

- N/A

Configuration Steps

Configuring the Syslog Suppression Rate

- (Optional) The configuration is performed on the AC. Run the **roaming logging rate-limit** command to configure the syslog suppression rate.
- Configure the syslog suppression rate. A larger rate configured indicates that more syslogs can be output per second.

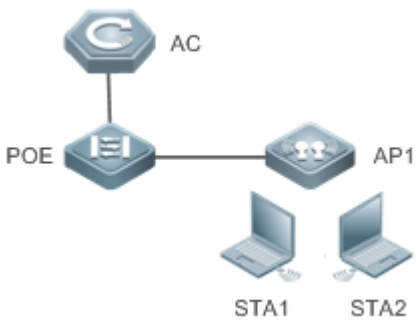
Command	**roaming logging rate-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the rate, which is expressed in records per seconds. The value ranges from 1 to 10000.
Defaults	By default, less than five syslog records are output per second, that is, the maximum syslog output rate is 5 records per second.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Suppressing STA Roaming Syslogs

Scenario **Figure 9-7**	

Configuration Steps	● Configure the STA syslog suppression rate.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# roaming logging rate-limit 30
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	AC# show running roaming logging rate-limit 30 !

Common Errors

- N/A

9.4.8 Preventing STA Roaming

Configuration Effect

- STAs are prevented from roaming within a WLAN.

Notes

- N/A

Configuration Steps

↘ Preventing STA Roaming within a WLAN

- (Optional) The configuration is performed on the AC. Run the **no roaming support wlan** command to prevent STA roaming.
- Roaming is permitted by default. Run the **no roaming support wlan** command to prevent STA roaming.

Command	[**no**] **roaming support wlan** *wlan-id*
Parameter Description	*wlan-id*: Specifies a WLAN.
Defaults	Roaming is permitted by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Preventing STA Roaming

Configuration Steps	• Configure roaming prevention within WLAN100.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# no roaming support wlan 100
Verification	• After the CAPWAP tunnel is established between an AP and an AC, check the configuration information.
AC	AC# show running no roaming support wlan 100 !

Common Errors

- N/A

9.5 Monitoring

Displaying

Description	Command
Displays configurations of all mobility groups.	**show mobility summary**
Displays configurations of a specified mobility group.	**show mobility status** *group-name*
Displays roaming statistics.	**show mobility statistics**
Displays roaming STA information.	**show mobility user** [*mac*]
Displays the roaming tracks of roaming STAs.	**show mobility user roam-track** *mac*

WLAN RF Configuration

1 Configuring RRM

1.1 Overview

Radio Resource Management (RRM) is an important feature running on an access controller (AC) for access point (AP) Radio Frequency (RF) management.

By analyzing the ambient RF environment of an AP in real time, RRM automatically adjusts the AP's working channel and transmit power based on a specific algorithm to avoid signal interference between APs and ensure normal operation of the wireless network.

When an AP is located in a complex RF environment, the AP may be severely interfered with. In this case, RRM can be enabled to improve user experience.

1.2 Applications

Application	Description
Centralized RRM	Multiple ACs constitute an RF group to provide centralized RRM for all APs in the entire network.

1.2.1 Centralized RRM

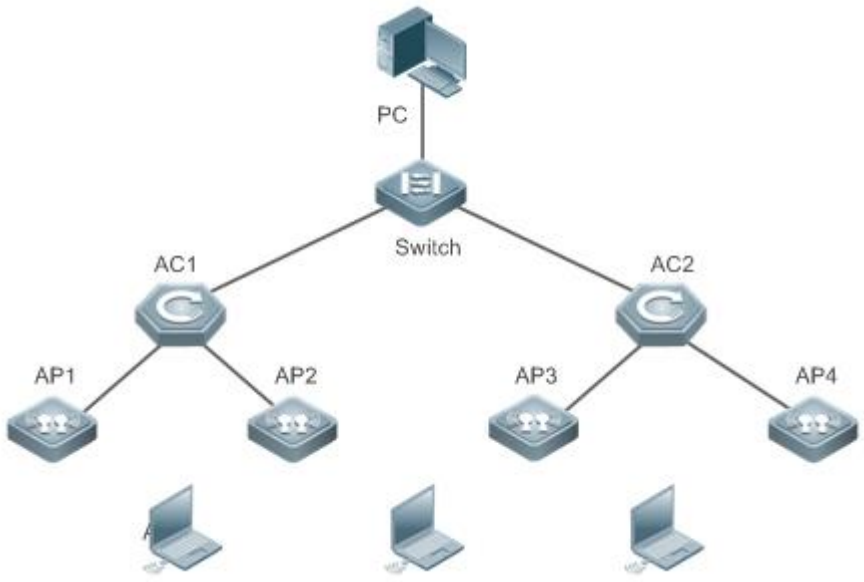
Scenario

Multiple ACs constitute an RF group to provide centralized RRM for all APs in the entire network.

Taking Figure 1-1 as an example, the clients are networked through APs which operate at the frequency band of 2.4 GHz. AP1, AP2, AP3 and AP4 are under centralized RRM within one RF group where Dynamic Channel Assignment (DCA) and Transmit Power Control (TPC) are enabled.

- A leader should be designated between AC1 and AC2, with the other being a member. The designated leader will implement centralized RRM.

Figure 1-1 Centralized RRM



Remarks	The switch is a core switch. AC 1 manages AP 1 and AP 2. AC 2 manages AP 3 and AP 4. AC 1 and AC 2 constitute an RF group.

Deployment

- With AC 1 being the leader and AC 2 being the member, configure AC 2 as the group member on AC 1 and configure AC 1 as the group leader on AC 2. The two ACs constitute an RF group.
- On the group leader AC 1, enable DCA and TPC to achieve centralized RRM.

1.3 Features

Basic Concepts

STA, AP and AC

STA: wireless station, a device with a wireless network interface card (WNIC), for example, a laptop or a cell phone.

AP: wireless access point, which provides wireless access for STAs.

AC: wireless controller, which is used to manage APs and provide wireless services.

RF Group

Multiple ACs constitute an RF group, with one AC designated as the leader which performs DCA and TPC for all APs.

RF Environment Information

- STA information: mainly includes STAs' Received Signal Strength Indication (RSSI) and Signal-to-Noise Ratio (SNR).
- Neighbor information: mainly includes neighboring APs' RSSI and working channels.
- Load: also known as utilization ratio, which is a percentage of the time spent by an AP in transmitting and receiving 802.11 data frames in the total time.
- Noise: noise intensity which affects normal reception of 802.11 signals. The unit is dBm.

- Interference: 802.11 signal interference and non-802.11 signal interference are included. The former comes from other APs and the latter generally comes from microwave radiations and Bluetooth devices. The unit is percentage (%).

Co-Channel Interference

When two APs close to each other are working in the same channel, co-channel interference occurs, which affects both APs' normal reception of 802.11 wireless packets.

Coverage Hole

When the transmit power of APs is so low that the AP signal strength in certain areas could not meet normal communication requirements, these areas are called coverage holes.

Overview

Feature	Description
RF Group	A leader-member relationship is established between ACs to form an RF group.
RF Environment Monitoring	The ambient RF environment of an AP is monitored in real time and the monitored data is sent to the AC for users to understand the AP's current RF environment.
DCA	The AC allocates an appropriate working channel to an AP based on the AP's ambient RF environment to reduce co-channel interference and improve user experience.
TPC	If multiple APs are close to each other and one of them features too high transmit power, the normal operation of other APs may be affected. In this case, the transmit power of the APs needs to be lowered to reduce the interference it generates.
Coverage Hole Detection and Correction	Through statistics and analysis of wireless signal characteristics, it can be determined whether a coverage hole exists. If a coverage hole exists, the transmit power can be increased for a specific AP to remedy the coverage hole.

1.3.1 RF Group

A leader-member relationship is established between ACs to form an RF group. A leader can perform centralized RRM for all APs only after the RF group is established between ACs. After an RF group including multiple ACs is established, RF resources can be assigned based on more comprehensive RF environment information, which is advantageous over a single AC.

Working Principle

ACs are connected through to establish an RF group, with the leader AC as the server and member ACs as the clients. After an RF group is established, when DCA or TPC is enabled, the leader requests each member for RF environment information. After connection, each member reports the information to the leader. The leader issues results to the members after completing algorithm execution.

Establishing an RF Group

Based on the configured IP address of the leader AC, each member AC periodically tries to establish a TCP connection with the leader AC. When a TCP connection is established, the leader queries whether the IP address of each member is on the group member list. If no, the leader cancels this connection. If yes, the TCP connection succeeds. A member sends an RF group registration request to the leader. If the registration succeeds, the leader returns a registration success

response to the member which is then successfully added to the group. Otherwise, a registration failure response is returned. The member disconnects from the leader after receiving the registration failure response.

↘ Maintaining the RF Group

When a member is successfully added to an RF group, keepalive packets are transmitted between the members and the leader periodically. When either party detects keepalive timeout, it cancels the connection. After disconnection, the member still tries to join a specified group periodically.

1.3.2 RF Environment Monitoring

APs monitor their ambient RF environment in real time and send the monitoring data to the associated AC. The RF environment information on each AP can be viewed on the AC.

Working Principle

The STA and neighbor information is obtained by APs through monitoring and analyzing wireless packets on the air interface, while the load, noise and interference information is obtained mainly by chip reading.

The AC notifies an AP to start collecting RF environment information. After information collection, the AP reports data to the AC.

1.3.3 DCA

For a single AP, DCA can prevent it from being subject to severe interference on the working channel.

For the global RF environment, reasonable channel assignment for each AP minimizes the interference among APs in the entire network and improves spectrum resource utilization and user experience.

Working Principle

If two APs close to each other work on the same channel, wireless signal conflict and interference occurs between them, which affect user experience.

DCA can comprehensively analyze all environmental factors (including neighbor information, loads, noises, and the number of STAs associated with an AP) and assign optimal working channels for all APs to solve channel conflict.

For example, if two APs work on the same channel or channels with frequency spectrum overlapped at the same time, the DCA algorithm can be used to stagger their channels to optimize the frequency spectrum.

1.3.4 TPC

TPC reduces signal interference between APs by reducing the APs' transmit power.

Working Principle

When an AP is powered on for the first time, the permissible maximum transmit power is used based on national or regional regulations. The higher the transmit power of an AP, the larger its signal coverage. If two adjacent APs have an excessive signal coverage overlap and work on the same frequency band, strong co-channel interference will be produced. TPC can determine whether the transmit power of an AP needs to be reduced or increased based on the information of each neighbor AP. When the co-channel interference between APs is too strong, if channels cannot be staggered, the only way to reduce the interference is to reduce the transmit power of both APs. When the interference is too little to ignore, the transmit power can be improved properly to enlarge signal coverage.

If DCA and TPC are both enabled, RRM considers the former first. If channels can be staggered, it is unnecessary to reduce the transmit power. Given this consideration, TPC uses the period set for DCA, and the TPC algorithm runs after the DCA algorithm.

1.3.5 Coverage Hole Detection and Correction

Through statistics and analysis of RSSI, it can be determined whether a coverage hole exists. If a coverage hole exists, you can increase the transmit power for a specific AP to correct the coverage hole.

Working Principle

Coverage Hole Detection (CHD) determines whether a coverage hole exists based on the quality of RSSI. This feature concerns only the data of STAs, and thus can operate independently on each AC.

When the SNR value of an STA is lower than a given threshold, the algorithm determines that a coverage hole exists. When the number of STAs in coverage holes exceeds a certain threshold (absolute number or proportion, which can be configured), the AC fixes coverage holes by improving the transmit power of APs.

1.4 Configuration

Configuration	Description and Command	
Configuring an RF Group	(Optional) It is used to configure an RF group that consists of multiple ACs.	
	advanced { 802.11a | 802.11b } group-leader	Configures the leader of an RF group.
	advanced { 802.11a | 802.11b } group-member	Configures a member of the RF group.
	network rf-network-name	Configures the name of an RF group.
Configuring RF Monitoring	(Optional) It is used to enable or disable RF environment monitoring and configure the monitoring parameters.	
	advanced { 802.11a | 802.11b } monitor mode	Enables RF environment monitoring.
	advanced { 802.11a | 802.11b } monitor channel-list	Configures the range of monitored channels.
	advanced { 802.11a | 802.11b } monitor coverage	Configures the period of client monitoring.
	advanced { 802.11a | 802.11b } monitor load	Configures the period of load monitoring.
	advanced { 802.11a | 802.11b } monitor noise	Configures the period of noise monitoring.
	advanced { 802.11a | 802.11b } monitor signal	Configures the period of neighbor monitoring.
Configuring DCA	(Optional) It is used to configure DCA.	
	advanced { 802.11a | 802.11b } channel global	Configures the DCA mode.
	advanced { 802.11a | 802.11b } channel add	Adds an optional channel to the DCA algorithm.
	advanced { 802.11a | 802.11b } channel delete	Deletes an optional channel from the DCA algorithm.

Configuration	Description and Command	
	advanced { 802.11a | 802.11b } channel clients	Configures the number threshold of clients using the DCA algorithm.
	advanced { 802.11a | 802.11b } channel countered-switch	Configures whether the DCA algorithm supports channel switching when an AP is countered.
	advanced { 802.11a | 802.11b } channel foreign	Configures whether interference is considered in the DCA algorithm.
	advanced { 802.11a | 802.11b } channel load	Configures whether loads are considered in the DCA algorithm.
	advanced { 802.11a | 802.11b } channel noise	Configures whether noises are considered in the DCA algorithm.
	advanced { 802.11a | 802.11b } channel pkt-loss-rate-threshold	Configures the threshold of packet-loss rate on the air interfaces used in the DCA algorithm.
	advanced { 802.11a | 802.11b } channel dca	Configures DCA parameters.
	advanced { 802.11a | 802.11b } channel update	Manually starts the DCA algorithm once.
Configuring TPC	(Optional) It is used to configure TPC parameters.	
	advanced { 802.11a | 802.11b } txpower dtpc	Enables or disables TPC.
	advanced { 802.11a | 802.11b } txpower global	Configures the TPC mode.
	advanced { 802.11a | 802.11b } txpower co-channel	Configures whether the TPC algorithm considers only neighbors on the same channel.
	advanced { 802.11a | 802.11b } txpower threshold	Configures the neighbor RSSI threshold used in the TPC algorithm.
	advanced { 802.11a | 802.11b } txpower update	Manually starts the TPC algorithm once.
Configuring Coverage Hole Detection and Correlation	(Optional) It is used to configure coverage hole detection and correction.	
	advanced { 802.11a | 802.11b } coverage	Enables or disables coverage hole detection and correction.
	advanced { 802.11a | 802.11b } coverage exception global	Configures the threshold of client failure rate used in the Coverage Hole Detection (CHD) algorithm.
	advanced { 802.11a | 802.11b } coverage level global	Configures the threshold of failed client number used in the CHD algorithm.
	advanced { 802.11a | 802.11b } coverage fail-rate	Configures the threshold of data or voice packet failure rate used in the CHD algorithm.
	advanced { 802.11a | 802.11b } coverage packet-count	Configures the threshold of failed data or voice packet number used in the CHD algorithm.

Configuration	Description and Command	
	advanced { 802.11a | 802.11b } coverage profile	Configures the SNR threshold of clients in a coverage hole used in the CHD algorithm.
	advanced { 802.11a | 802.11b } coverage rssi-threshold	Configures the RSSI threshold of data or voice packets used in the CHD algorithm.
Configuring RRM Logging	(Optional) It is used to configure the RRM logging feature.	
	advanced { 802.11a | 802.11b } logging channel	Enables or disables DCA logging.
	advanced { 802.11a | 802.11b } logging txpower	Enables or disables TPC logging.
	advanced { 802.11a | 802.11b } logging coverage	Enables or disables logging on over-limit AP clients.
	advanced { 802.11a | 802.11b } logging foreign	Enables or disables logging on over-limit AP interference.
	advanced { 802.11a | 802.11b } logging load	Enables or disables logging on over-limit AP loads.
	advanced { 802.11a | 802.11b } logging noise	Enables or disables logging on over-limit AP channel noises.
	advanced { 802.11a | 802.11b } logging performance	Enables or disables logging on over-limit AP performance.
	advanced { 802.11a | 802.11b } profile clients	Configures the alarm threshold of the AP client number.
	advanced { 802.11a | 802.11b } profile foreign	Configures the alarm threshold of AP interference.
	advanced { 802.11a | 802.11b } profile noise	Configures the alarm threshold of AP channel noises.
	advanced { 802.11a | 802.11b } profile throughput	Configures the alarm threshold of AP data throughput.
	advanced { 802.11a | 802.11b } profile utilization	Configures the alarm threshold of AP utilization.

1.4.1 Configuring an RF Group

Configuration Effect

- Use multiple ACs to form an RF group and choose a leader AC to uniformly implement DCA and TPC.

Notes

- If an AC is not included as a member in any RF group, this AC takes itself as the leader by default to independently manage RF resources of its associated APs.
- If an AC is configured as the group leader, it cannot be configured as a member, and vice versa.
- The first IP address of the local Loopback0 interface is used for the communication between ACs in an RF group.

Configuration Steps

Configuring an RF Group

- (Optional) Configure an RF group with multiple ACs and specify one AC as the leader to implement centralized management on RF resources (including AP channels and transmit power).
- Specify one AC as the group leader, add an IP list of admissible members on this AC, and configure the IP address of the group leader on member ACs.
- Run the **advanced** { **802.11a** | **802.11b** } **group-member** command to configure IP addresses of the member ACs. To specify one AC as the group leader, a member IP list needs to be configured on this AC. Only ACs on the member IP list can be added to the RF group.
- Run the **advanced** { **802.11a** | **802.11b** } **group-leader** command to specify an IP address as the RF group leader.
- Run the **network rf-network-name** command to configure the RF group name.

By default, an AC takes itself as the group leader to independently manage RF resources of its associated APs.

Command	**advanced** { **802.11a**	**802.11b** } **group-member** *ip-address*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *ip-address*: IP address of an RF group member
Defaults	No RF group member is configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **group-leader** *ip-address*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *ip-address*: IP address of an RF group leader
Defaults	An AC takes itself as the RF group leader to independently manage RF resources of its associated APs.
Command Mode	Global configuration mode
Usage Guide	N/A

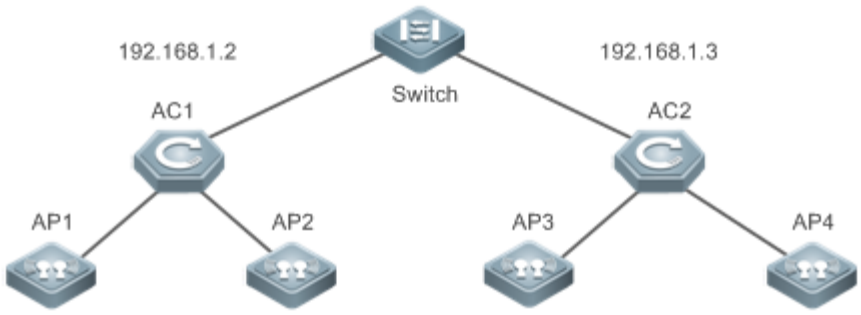
Command	**network rf-network-name** *group-name*
Parameter Description	*group-name*: RF group name
Defaults	The default group name is rf-network
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **group** command on the leader AC and member ACs respectively to verify the established RF group.

Configuration Example

Establishing an RF Group with Two ACs

Scenario **Figure 1-2**	
Configuration Steps	● Configure the Loopback0 addresses of AC1 and AC2 as 192.168.1.2 and 192.168.1.3 respectively, and ensure that the ping command is successful between the two ACs. ● Take AC1 as the RF group leader and add a member whose IP address is 192.168.1.3 on AC1. Take AC2 as a member and add the IP address 192.168.1.2 of the group leader on AC2.
AC1	AC1#configure terminal AC1(config)#interface loopback 0 AC1(config-if-Loopback 0)#ip address 192.168.1.2 255.255.255.0 AC1(config-if-Loopback 0)#exit AC1(config)#advanced 802.11b group-member 192.168.1.3 AC1(config)#exit
AC2	AC2#configure terminal AC2(config)#interface loopback 0 AC2(config-if-Loopback 0)#ip address 192.168.1.3 255.255.255.0 AC2(config-if-Loopback 0)#exit AC2(config)#advanced 802.11b group-leader 192.168.1.2 AC2(config)#exit
Verification	View the RF group status on AC1 and AC2 respectively to determine whether the RF group is successfully established.
AC1	AC1#show advanced 802.11b group RF Group Information Radio Type ..... 802.11b RF Group Name ..... rf-network I'm leader ..... yes

	Group member ..... 192.168.1.3 (connected) Last Run ..... 15 seconds ago
AC2	AC2#show advanced 802.11b group RF Group Information Radio Type ..... 802.11b RF Group Name ..... rf-network I'm leader ..... no Group leader ..... 192.168.1.2 (connected) Last Run ..... 15 seconds ago

Common Errors

- The network between ACs is blocked, which causes failed RF grouping.
- The IP address of the group leader is configured on a member, but the IP address of the member is not added on the leader, which causes failed RF grouping.
- The RF group is named inconsistently, which causes failed RF grouping.

1.4.2 Configuring RF Environment Monitoring

Configuration Effect

- A target AP's RF environment information can be viewed on the AC.

Notes

- N/A

Configuration Steps

RF Environment Monitoring

- (Optional) Configure RF environment monitoring to view a target AP's RF environment information.
- Enable RF environment monitoring on an AC and specify the monitoring period for each indicator.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor mode** { **enable** | **disable** } command to enable or disable RF environment monitoring. Because the collection of RF environment information takes up a small portion of an AP's normal operation time, enabling RF environment monitoring slightly reduces AP performance.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor channel-list** command to configure the range of monitored channels.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor coverage** command to configure the period of client monitoring.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor load** command to configure the period of load monitoring.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor noise** command to configure the period of noise monitoring.
- Run the **advanced** { **802.11a** | **802.11b** } **monitor signal** command to configure the period of neighbor monitoring.

Command	**advanced** { **802.11a** | **802.11b** } **monitor mode** { **enable** | **disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: Enables RF environment monitoring. **Disable**: Disables RF environment monitoring.
Defaults	RF environment monitoring is disabled.
Command Mode	Global configuration mode.
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **monitor channel-list** { **all** | **country** | **dca** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **all**: Monitors all channels. **country**: Monitors channels within a specified country. **dca**: Monitors channels used by the DCA algorithm.
Defaults	The default value is **country**.
Command Mode	Global configuration mode.
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **monitor coverage** *interval*
Parameter Description	**802.11a**: 5 GHz network. **802.11a**: 2.4 GHz network. *interval*: Specifies the period of client monitoring.
Defaults	The period of client monitoring is 180 seconds.
Command Mode	Global configuration mode.
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **monitor load** *interval*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *interval*: Specifies the period of load monitoring
Defaults	The period of load monitoring is 60 seconds.
Command Mode	Global configuration mode.
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **monitor noise** *interval*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *interval*: Specifies the period of noise monitoring.

Defaults	The period of noise monitoring is 180 seconds.
Command Mode	Global configuration mode.
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **monitor signal** *interval*
Parameter Description	**802.11a**: 5 GHz network. **802.11a**: 2.4 GHz network. *interval*: Specifies the period of neighbor monitoring.
Defaults	The period of neighbor monitoring is 180 seconds.
Command Mode	Global configuration mode.
Usage Guide	N/A

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **monitor** command to display RF environment monitoring parameters.
- Run the **show ap auto-rf** command to display AP RF environment information.

Configuration Example

Enabling RF Environment Monitoring

Configuration Steps	Enable RF environment monitoring.
AC	`AC#configure terminal` `AC(config)#advanced 802.11b monitor mode enable` `AC(config)#exit`
Verification	Run the **show ap auto-rf radio** *radio-id ap-name* command to display AP RF environment information on the target AC.

Common Errors

- N/A

1.4.3 Configuring DCA

Configuration Effect

- Enable DCA on an AC so that the AC can assign appropriate working channels for APs based on AP RF environment information improving user experience.

Notes

- Normally, it is not recommended to set the period of DCA too short. By default, DCA is performed once every 20 minutes.
- If an AC joins an RF group as a member, the working channel of this member will be adjusted by the uniform channel assignment on the leader AC.
- If a channel is manually configured on an AP, DCA will not be conducted for this AP.

Configuration Steps

Configuring DCA

- (Optional) Configure DCA to automatically assign proper working channels for APs.
- Enable DCA on the target AC and configure its running mode as periodic mode or trigger mode based on your demand.
- Run the **advanced** { **802.11a** | **802.11b** } **channel global** command to configure the DCA mode. By default, DCA is running in AUTO mode.

DCA has three running modes: AUTO, ONCE and OFF. AUTO is the periodic mode in which the AC periodically assigns proper working channels for all APs. ONCE is the trigger mode in which the AC usually performs channel assignment once when the AP and AC are connected for the first time. When the channel property of the AP changes from Manual to Global, channel assignment is triggered once again. OFF is the disabled mode in which the AC does not perform DCA for APs.

- Run the **advanced** { **802.11a** | **802.11b** } **channel** { **add** | **delete** } command to add or delete an optional channel to or from DCA.
- Run the **advanced** { **802.11a** | **802.11b** } **channel clients** command to configure the number threshold of clients using the DCA algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **channel countered-switch** command to configure whether the DCA algorithm supports channel switching when an AP is countered.
- Run the **advanced** { **802.11a** | **802.11b** } **channel foreign** command to configure whether interference is considered in the DCA algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **channel noise** command to configure whether noises are considered in the DCA algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **channel pkt-loss-rate-threshold** command to configure the threshold of packet-loss rate on the air interfaces used in the DCA algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **channel dca anchor-time** command to configure when the DCA algorithm is enabled and ends within a day.
- Run the **advanced** { **802.11a** | **802.11b** } **channel dca chan-width-11n** command to configure the frequency bandwidth used by the DCA algorithm in an 802.11n network.
- Run the **advanced** { **802.11a** | **802.11b** } **channel dca interval** command to configure the running period for the DCA algorithm, which takes effect only when DCA is configured to the AUTO mode. The shorter the cycle, the faster the AP channel assignment. APs are required to scan ambient RF environment information before channel assignment, and some air interface resources will be occupied; therefore, it is normally not recommended to set the assignment period too short.

- Run the **advanced** { **802.11a** | **802.11b** } **channel dca period** command to configure the running time of the DCA algorithm within a week.
- Run the **advanced** { **802.11a** | **802.11b** } **channel dca sensitivity** command to configure the sensitivity of the DCA algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **channel update** command to manually start the DCA algorithm once.

Command	**advanced** { **802.11a**	**802.11b** } **channel global** { **auto**	**off**	**once** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **auto**: Periodic mode. **once**: Trigger mode. **off**: Disabled mode.
Defaults	DCA runs in periodic mode (AUTO).
Command Mode	Global configuration mode.
Usage Guide	In periodic mode, appropriate working channels are assigned to APs periodically, while in trigger mode, the working channel assignment is conducted once only when an AP is online for the first time or the AP's channel property is modified from Manual to Global.

Command	**advanced** { **802.11a**	**802.11b** } **channel** { **add**	**delete** } *channel-id*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **add**: Adds an optional channel to DCA. **delete**: Deletes an optional channel from DCA. *channel-id*: Channel ID
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **channel clients** *clients-num*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *clients-num*: Specifies the number threshold of clients using the DCA algorithm.
Defaults	The default value is 0, which means that channel assignment is not conducted when clients are associated with an AP.
Command Mode	Global configuration mode
Usage Guide	Channel switching may lead to user re-association; therefore, when the number of users associated with an AP exceeds this threshold, channel assignment will not be conducted for this AP.

Command	**advanced** { **802.11a**	**802.11b** } **channel countered-switch** { **enable**	**disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network

	enable: Enables channel switching when an AP is countered. **disable**: Disables channel switching when an AP is countered.
Defaults	Channel switching is disabled when an AP is countered.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **channel foreign** { **enable** | **disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: Considers AP interference in the DCA algorithm. **disable**: Ignores AP interference in the DCA algorithm.
Defaults	AP interference is considered in the DCA algorithm.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **channel noise** { **enable** | **disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: Considers noise factors in the DCA algorithm. **Disable**: Ignores noise factors in the DCA algorithm.
Defaults	Noise factors are considered in the DCA algorithm.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **channel pkt-loss-rate-threshold** *threshold*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *threshold*: Specifies the threshold of packet-loss rate on the air interfaces used in the DCA algorithm.
Defaults	The default value is 100, which means that the packet-loss rate on the air interfaces is ignored in the DCA algorithm.
Command Mode	Global configuration mode
Usage Guide	When the DCA algorithm conducts channel selection, if the packet-loss rate on the air interfaces for the current working channel is found to exceed the threshold, channel switching will be conducted.

Command	**advanced** { **802.11a** | **802.11b** } **channel dca anchor-time** *start duration*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *start*: Specifies the time when the DCA algorithm starts running in a day. The unit is hour and the value ranges from 0 to 23. *duration*: Specifies the time duration when the DCA algorithm keeps running. The unit is hour and the

	value ranges from 1 to 24.
Defaults	The default value of start-hour is 2 and that of duration is 2, meaning that the DCA algorithm runs from 2:00 am to 4:00 am.
Command Mode	Global configuration mode
Usage Guide	When the DCA algorithm is set to run in periodic mode, DCA is conducted only in this time frame. For example, if DCA is expected to run from 2:00 am to 4:00 am, you can run the **advanced** { **802.11a** | **802.11b** } **channel dca anchor-time 2 2** command.

Command	**advanced** { **802.11a** | **802.11b** } **channel dca chan-width-11n** { **20** | **40** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **20**: Uses 20 MHz bandwidth **40**: Uses 40 MHz bandwidth
Defaults	20 MHz bandwidth is used.
Command Mode	Global configuration mode
Usage Guide	20 MHz or 40 MHz bandwidth are supported.

Command	**advanced** { **802.11a** | **802.11b** } **channel dca interval** *interval*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *interval*: Period of the DCA algorithm
Defaults	The DCA algorithm runs once every 20 minutes.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **channel dca period** *day1* **to** *day2*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *day1*: Specifies which day of a week the DCA algorithm starts on. *day2*: Specifies which day of a week the DCA algorithm stops on (including that day).
Defaults	The DCA algorithm runs throughout a week, from Sunday to Saturday.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **channel dca sensitivity** { **low** | **medium** | **high** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **low**: The DCA algorithm is not very sensitive to algorithm environment change. **medium**: The DCA algorithm is of medium sensitivity to RF environment change. **high**: The DCA algorithm is very sensitive to RF environment change.

Defaults	The DCA algorithm is of medium sensitivity to RF environment change.
Command Mode	Global configuration mode.
Usage Guide	Higher sensitivity means faster channel assignment.

Command	**advanced** { **802.11a** | **802.11b** } **channel update**
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network
Defaults	**N/A**
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **channel** command to display DCA status.
- Run the **show ap-config summary** command to display the channel assignment result of an AP.

Configuration Example

Configuring the DCA Parameters

Configuration Steps	Configure DCA in periodic mode and set the period to 30 minutes.
AC	`AC#configure terminal` `AC(config)#advanced 802.11b channel global auto` `AC(config)#advanced 802.11b channel dca interval 30` `AC(config)#exit`
Verification	Display DCA status.
AC	`AC#show advanced 802.11b channel` `Automatic Channel Assignment` `Radio Type..... 802.11b` `Channel Assignment Mode..... AUTO` `Channel Update Interval..... 1800 seconds` `Periodic Motion (Day of A Week)..... All days` `Anchor Time (Hour of The Day)..... 2` `The Duration of DCA (By Hour)..... 2` `Consider Foreign Factor..... yes` `Consider Load Factor..... no`

```
Consider Noise Factor..... no
Switch Channel When Countered..... disable
Packet Loss Rate Threshold.....100%
Clients Threshold..... 0 client
Channel Assignment Leader..... 192.168.1.2
Last Run..... 263 seconds ago
DCA Sensitivity Level..... MEDIUM (15 dB)
DCA 802.11n Channel Width..... 20 MHz
Auto-RF Allowed Channel List..... 1,6,11
Auto-RF Unused Channel List..... 2,3,4,5,7,8,9,10,12,13
```

Common Errors

- If an AP has been manually assigned a channel, DCA will not be conducted for this AP.

1.4.4 Configuring TPC

Configuration Effect

- After TPC is enabled, the AC configures proper transmit power for APs based on the APs' RF environment information to reduce the co-channel interference between the APs.

Notes

- TPC is aimed at reducing the co-channel interference caused by an AP to other APs, and therefore, the TPC algorithm needs to realize the degree of co-channel interference from other APs to determine whether power control is required. Currently, TPC is supported on Ruijie APs only. If these APs are associated with multiple ACs, the ACs need to be in the same RF group.

Configuration Steps

Configuring TPC

- (Optional) Configure TPC to automatically control the transmit power of APs to avoid intensive interference between these APs.
- Enable TPC on the target AC, and configure it to run in periodic mode, trigger mode or constant power mode based on your demand.
- Run the **advanced** { **802.11a** | **802.11b** } **txpower dtpc** { **enable** | **disable** } command to enable or disable TPC.
- Run the **advanced** { **802.11a** | **802.11b** } **txpower global** command to configure the TPC mode.

TPC has three running modes: constant power mode, periodic mode (AUTO) and trigger mode (ONCE). In constant power mode, a power level is manually specified for each AP connected to the AC, with level 1 being the highest transmit power and level 8 being the lowest transmit power, and the transmit power on a level is 50% of that on the next level, with the level ranging from 1 to 8; in periodic mode (AUTO), the AC periodically conducts TPC for all APs; in trigger mode (ONCE), power control is conducted once only when an AP is connected with the AC for the first time or when the AP's power property changes from Manual to Global.

- Run the **advanced** { **802.11a** | **802.11b** } **txpower co-channel** command to configure whether the TPC algorithm considers only neighbors on the same channel.
- Run the **advanced** { **802.11a** | **802.11b** } **txpower threshold** command to configure the threshold of neighbor RSSI used in the TPC algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **txpower update** command to manually start the TPC algorithm once.

Command	**advanced** { **802.11a**	**802.11b** } **txpower dtpc** { **enable**	**disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: enables TPC **disable**: disables TPC
Defaults	TPC is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **txpower global** { **auto**	**once**	*power-level* }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **auto**: Periodic mode. **once**: Trigger mode. *level*: Specifies power levels for all APs, ranging from 1 to 8, with a smaller value indicating a higher power level.
Defaults	TPC runs in periodic mode (AUTO).
Command Mode	Global configuration mode
Usage Guide	The parameters configured with this command take effect only when TPC is enabled. The TPC algorithm runs after the DCA algorithm, and therefore, the period set for DCA is used.

Command	**advanced** { **802.11a**	**802.11b** } **txpower co-channel** { **enable**	**disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: Only neighbor APs on the same channel are considered in the TPC algorithm. **disable**: All neighbor APs are considered in the TPC algorithm.
Defaults	All neighbor APs are considered in the TPC algorithm.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **txpower threshold** *value*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network

	value: Specifies the threshold of neighbor RSSI, ranging from -90 dBm to -50 dBm
Defaults	The threshold of neighbor RSSI is -60 dBm.
Command Mode	Global configuration mode
Usage Guide	The smaller the neighbor RSSI threshold, the easier the power control is triggered to reduce an AP's transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **txpower update**
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network
Defaults	**N/A**
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **txpower** command to display TPC status.
- Run the **show ap-config summary** command to display the power control result of an AP.

Configuration Example

Configuring TPC Parameters

Configuration Steps	Enable TPC and configure it to run in periodic mode.
AC	`AC#configure terminal` `AC(config)#advanced 802.11b txpower dtpc enable` `AC(config)#advanced 802.11b txpower global auto` `AC(config)#exit`
Verification	Display TPC status.
AC	`AC#show advanced 802.11b txpower` `Automatic Transmit Power Assignment` `Radio Type..... 802.11b` `Dynamic Transmit Power Control Support..... enable` `Transmit Power Assignment Mode..... AUTO` `Transmit Power Update Interval..... 1800 seconds` `Consider The Same Channel Neighbor Only..... No` `Transmit Power Threshold..... -60 dBm`

	Transmit Power Neighbor Count..... 3 APs Transmit Power Assignment Leader..... 192.168.1.2 Last Run..... 568 seconds ago

Common Errors

- If an AP is manually assigned a power level, TPC will not be conducted for this AP.

1.4.5 Configuring Coverage Hole Detection and Correction

Configuration Effect

- After coverage hole detection and correction is enabled, the AC determines whether an AP has a coverage hole. If yes, the AP's transmit power will be increased to correct the coverage hole.

Notes

- The coverage hole detection and correction feature needs only statistic information on STAs associated with this AP, and therefore, it can operate independently on a single AC and is independent of any RF group.

Configuration Steps

↘ Configuring Coverage Hole Detection and Correction

- (Optional) Configure coverage hole detection and correction to enable APs to actively detect and correct coverage holes.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage** { **enable** | **disable** } command to enable or disable coverage hole detection and correction.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage exception global** command to configure the threshold of client failure rate used in the CHD algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage level global** command to configure the threshold of failed client number used in the CHD algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage** { **data** | **voice** } **fail-rate** command to configure the threshold of data or voice packet failure rate used in the CHD algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage** { **data** | **voice** } **packet-count** command to configure the threshold of failed data or voice packet number used in the CHD algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage profile** command to configure the SNR threshold of clients in a coverage hole used in the CHD algorithm.
- Run the **advanced** { **802.11a** | **802.11b** } **coverage** { **data** | **voice** } **rssi-threshold** command to configure the RSSI threshold of data or voice packets used in the CHD algorithm.

Command	**advanced** { **802.11a**	**802.11b** } **coverage** { **enable**	**disable** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **enable**: Enables coverage hole detection and correction. **disable**: Disables coverage hole detection and correction.

Defaults	Coverage hole detection and correction is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **coverage exception global** *percent*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *percent*: Specifies the threshold percentage of failed clients, ranging from 1 to 100.
Defaults	The default value is 25.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **coverage level global** *clients-num*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *clients-num*: Specifies the threshold of failed client number, ranging from 1 to 75.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **coverage** { **data** | **voice** } **fail-rate** *percent*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **data**: Specifies the threshold for data packets. **voice**: Specifies the threshold for voice packets. *percent*: Specifies the threshold percentage of failed packets, ranging from 1 to 100.
Defaults	The default value is 20.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **coverage** { **date** | **voice** } **packet-count** *packets*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **data**: Specifies the threshold for data packets.

	voice: Specifies the threshold for voice packets. *percent*: Specifies the threshold number of failed packets, ranging from 1 to 255.
Defaults	The default value is 10.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **coverage profile** *value*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network *value*: SNR threshold of clients in a coverage hole, ranging from 1 dB to 30 dB.
Defaults	The default value for a 5 GHz network is 16 dB, and the default value for a 2.4 GHz network is 12 dB.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Command	**advanced** { **802.11a** | **802.11b** } **coverage** { **data** | **voice** } **rssi-threshold** *value*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **data**: Specifies the threshold for data packets. **voice**: Specifies the threshold for voice packets. *value*: RSSI threshold, ranging from -90 to -60 .
Defaults	The default value for data packets is -80 dBm, and the default value for voice packets is -75 dBm.
Command Mode	Global configuration mode
Usage Guide	The smaller the value is, the easier the coverage hole correction is triggered to increase APs' transmit power.

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **coverage** command to display the status of coverage hole detection and correction.
- Run the **show ap-config summary** command to display the power change result of an AP.

Configuration Example

Configuring Coverage Hole Detection and Correction

Configuration Steps	Enable coverage hole detection and correction.
AC	`AC#configure terminal`

	AC(config)#advanced 802.11b coverage enable AC(config)#exit
Verification	Display the status of coverage hole detection and correction.
AC	AC#show advanced 802.11b coverage Coverage Hole Detection Radio Type..... 802.11b Coverage Hole Detection Mode..... enable Coverage Voice Packet Count..... 10 packets Coverage Voice Packet Percentage..... 20% Coverage Voice RSSI Threshold..... -75 dBm Coverage Data Packet Count..... 10 packets Coverage Data Packet Percentage..... 20% Coverage Data RSSI Threshold..... -80 dBm Global Coverage Exception Level..... 25% Global Client Minimum Exception Level..... 3 clients Global Coverage Profile Value..... 12 dB

Common Errors

- If a power level has been manually specified for an AP, CHD will not increase the AP's transmit power.

1.4.6 Configuring RRM Logging

Configuration Effect

- Enable RRM logging to print RRM logs on the target AC.

Notes

- If an AC manages too many APs, enabling RRM logging may cause too much information to be printed.

Configuration Steps

↘ Enabling or Disabling RRM Logging

- (Optional) Enable RRM logging to view RRM logs on the target AC.
- RRM logging provides log classification, allowing you to enable or disable certain logs on the AC.
- Run the **advanced** { **802.11a** | **802.11b** } **logging channel** { **on** | **off** } command to enable or disable DCA logging.
- Run the **advanced** { **802.11a** | **802.11b** } **logging txpower** { **on** | **off** } command to enable or disable TPC logging.
- Run the **advanced** { **802.11a** | **802.11b** } **logging coverage** { **on** | **off** } command to enable or disable the logging on over-limit AP clients.

- Run the **advanced** { **802.11a** | **802.11b** } **logging load** { **on** | **off** } command to enable or disable logging on over-limit AP loads.
- Run the **advanced** { **802.11a** | **802.11b** } **logging performance** { **on** | **off** } command to enable or disable logging on over-limit AP data throughput.
- Run the **advanced** { **802.11a** | **802.11b** } **logging foreign** { **on** | **off** } command to enable or disable logging on over-limit AP interference.
- Run the **advanced** { **802.11a** | **802.11b** } **logging noise** { **on** | **off** } command to enable or disable logging on over-limit AP channel noises.

Command	**advanced** { **802.11a**	**802.11b** } **logging channel** { **on**	**off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **logging txpower** { **on**	**off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **logging coverage** { **on**	**off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a**	**802.11b** } **logging load** { **on**	**off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.

Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **logging performance** { **on** | **off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **logging foreign** { **on** | **off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**advanced** { **802.11a** | **802.11b** } **logging noise** { **on** | **off** }
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **on**: Enables logging. **off**: Disables logging.
Defaults	Logging is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring RRM Alarm Thresholds

- (Optional) Alarm thresholds can be configured to trigger RRM logging on the target AC.
- Alarm thresholds can be configured to monitor various data (including the number of STAs associated with an AP, load, throughput, interference, and noise) on the target AC. If an indicator exceeds the set alarm threshold and the corresponding logging is enabled, RRM log printing is triggered.
- Run the **advanced** { **802.11a** | **802.11b** } **profile clients** command to configure the alarm threshold of the AP client number.
- Run the **advanced** { **802.11a** | **802.11b** } **profile utilization** command to configure the alarm threshold of AP loads.

- Run the **advanced** { **802.11a** | **802.11b** } **profile throughput** command to configure the alarm threshold of AP data throughput.
- Run the **advanced** { **802.11a** | **802.11b** } **profile foreign** command to configure the alarm threshold of AP interference.
- Run the **advanced** { **802.11a** | **802.11b** } **profile noise** command to configure the alarm threshold of AP channel noises.

Command	**advanced** { **802.11a**	**802.11b** } **profile clients** { **global**	*ap-name* } *clients-num*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **global**: Global alarm threshold *ap-name*: Alarm threshold for a specified AP *clients-num*: Alarm threshold of the number of clients
Defaults	The default value is 32.
Command Mode	Global configuration mode
Usage Guide	If an AP's alarm threshold of the number of clients is specified, the global alarm threshold will not be used.

Command	**advanced** { **802.11a**	**802.11b** } **profile utilization** { **global**	*ap-name* } *percent*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **global**: Global alarm threshold *ap-name*: Alarm threshold for a specified AP *percent*: Load alarm threshold
Defaults	The default value of *percent* is 80%.
Command Mode	Global configuration mode
Usage Guide	If an AP's alarm threshold is specified, the global alarm threshold will not be used.

Command	**advanced** { **802.11a**	**802.11b** } **profile throughput** { **global**	*ap-name* } *value*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **global**: Global alarm threshold *ap-name*: Alarm threshold for a specified AP *value*: alarm Threshold of AP data throughput
Defaults	The default *value* is 150,000,000 bps.
Command Mode	Global configuration mode
Usage Guide	If an AP's alarm threshold is specified, the global alarm threshold will not be used.

Command	**advanced** { **802.11a**	**802.11b** } **profile foreign** { **global**	*ap-name* } *percent*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network

	global: Global alarm threshold *ap-name*: Alarm threshold for a specified AP *percent*: Alarm threshold of AP interference
Defaults	The default *percent* is 60%.
Command Mode	Global configuration mode
Usage Guide	If an AP's alarm threshold is specified, the global alarm threshold will not be used.

Command	**advanced** { **802.11a** | **802.11b** } **profile noise** { **global** | *ap-name* } *value*
Parameter Description	**802.11a**: 5 GHz network **802.11a**: 2.4 GHz network **global**: Global alarm threshold *ap-name*: Alarm threshold for a specified AP *value*: Alarm threshold of channel noises
Defaults	The default *value* is -70 dBm.
Command Mode	Global configuration mode
Usage Guide	If an AP's alarm threshold is specified, the global alarm threshold will not be used.

Verification

- Run the **show advanced** { **802.11a** | **802.11b** } **logging** command to check whether RRM logging is enabled.
- Run the **show advanced** { **802.11a** | **802.11b** } **profile** command to check the configured alarm thresholds.
- Observe whether RRM logs are printed on the target AC in a period of time.

Configuration Example

Configuring RRM Logging

Configuration Steps	Enable DCA and TPC logging.
AC	AC#configure terminal AC(config)#advanced 802.11b logging channel on AC(config)#advanced 802.11b logging txpower on AC(config)#exit
Verification	Display RRM logging information.
AC	AC#show advanced 802.11b logging RF Event and Performance Logging Radio Type..... 802.11b Channel Update Logging..... On

```
TxPower Update Logging..... On
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
```

Common Errors

- N/A

1.5 Monitoring

Displaying

Description	Command
Displays RF group status.	**show advanced** { **802.11a** | **802.11b** } **group**
Displays RF environment monitoring status.	**show advanced** { **802.11a** | **802.11b** } **monitor**
Displays the RF environment information of an AP.	**show ap auto-rf radio** *radio-id ap-name*
Displays DCA status.	**show advanced** { **802.11a** | **802.11b** } **channel**
Displays TPC status.	**show advanced** { **802.11a** | **802.11b** } **txpower**
Displays the status of coverage hole detection and correction.	**show advanced** { **802.11a** | **802.11b** } **coverage**
Displays whether RRM logging is enabled.	**show advanced** { **802.11a** | **802.11b** } **logging**
Displays RRM alarm thresholds.	**show advanced** { **802.11a** | **802.11b** } **profile**
Displays AP channels and transmit power.	**show advanced** { **802.11a** | **802.11b** } **summary**

2 Configuring WLAN Optimization

2.1 Overview

Wireless network optimization is to optimize the wireless network and enhance the experience of wireless users by adjusting some configuration of the WLAN.

WLAN configuration can be optimized to:

- Reduce co-channel interference and adjacent-channel interference and enhance signal coverage.
- Increase the channel bandwidth.
- Improve the channel utilization rate.
- Improve the available channel bandwidth for wireless users.
- Decrease network attacks and multicast packet bandwidth usage.
- Improve the downlink throughput of the AP.
- Reduce weak-signal terminals and overall wireless network performance.
- Reduce the influence of the power-saving network adapter.
- Limit the number of access users.

Different WLAN optimization methods are applicable to different application scenarios. See the following table.

WLAN Optimization Method	Application Scenario
Channel planning and adjustment	This method is used as required.
Power planning and adjustment	This method is used as required.
Terminating low-rate applications	This method is applicable to the high-density deployment scenario (school and building).
Establishing a pure 11n wireless network	Settings shall be performed based on actual network requirements.
Adjusting Beacon sending interval	This method is applicable to the high-density deployment scenario where many service set identifiers (SSIDs) are configured for the AP.
Enabling layer 2 isolation for wireless users in a VLAN	This function must be configured for the network not requiring layer 2 mutual-access.
Enabling the RTS/CTS protection mechanism	This method is applicable to the network involving indoor coverage.
Enhancing the AP's packet sending priority and suppressing packet sending by the wireless client	It is recommended that you determine whether to use this method based on actual effects.
Reducing the influence of weak-signal terminals	This method is applicable to the high-density deployment scenario (school and building).
Band selection	This method is applicable to the high-density deployment scenario where the AP supports dual bands.
Power-saving client processing optimization	This method is applicable to all scenarios.

WLAN Optimization Method	Application Scenario
11N A-MPDU aggregation frame sending protection	This method is applicable to all scenarios.
Limiting the STA number on the AP	This method is applicable to the high-density deployment scenario (school and building) with lots of wireless users.

Protocol Specification

- IEEE Std 802.11-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

2.2 Applications

Typical Application	Scenario
802.11n	AP and STA both support the 11n network.
WLAN Spectrum Navigation of Fit AP	Fit AP architecture. The spectrum navigation function is enabled for the WLAN composed of multiple dual-band APs.

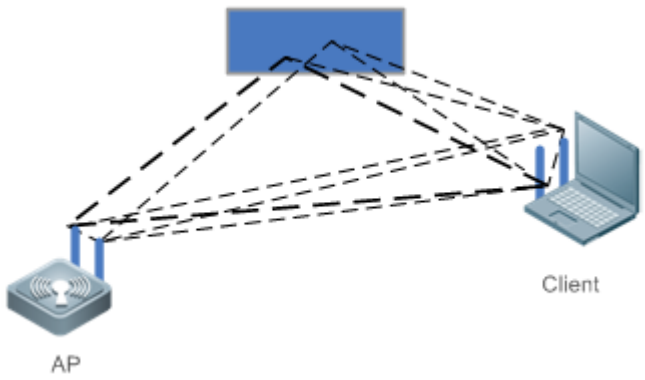
2.2.1 802.11n

Scenario

As a new protocol of the 802.11 protocol family, 802.11n supports two frequency bands, that is, 2.4 GHz and 5 GHz. It aims to provide WLAN access users with higher access rate. 802.11n improves the communication rate by using the MIMO technology or by increasing the bandwidth and improving the channel utilization rate.

As shown in Figure 2-1, the client accesses the wired network through the AP; the client and AP communicate with each other in wireless mode; and there are multiple transmission paths between the client and AP.

Figure 2-1



Remarks	AP represents a wireless access point. Client represents a wireless client.

Deployment

- Enable the IEEE802.11 protocol on the AP and Client to implement access and authentication of the wireless client.

2.2.2 Spectrum Navigation for WLAN Composed of Fit APs

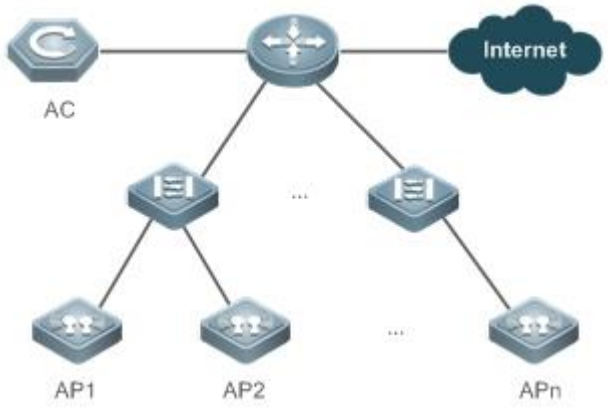
Scenario

Fit AP architecture. The spectrum navigation function is enabled for the WLAN composed of multiple dual-band APs.

As shown in Figure 2-2:

- One AC is associated with many dual-band APs. The AC and APs are connected by the layer 2 switching device and layer 3 routing device.
- WLAN is mapped to the two radio frequency (RF) interfaces of all dual-band APs.

Figure 2-2



Remarks	AC represents a wireless access controller. AP1, AP2… and APn are all dual-band APs.

Deployment

- Manage the operating parameters of the spectrum navigation function on the AC device.
- Enable the spectrum navigation function on the AP device to identify the STA type and guide STA access.

2.3 Features

Basic Concepts

WLAN

Wireless Local Area Network (WLAN) interconnects computer devices by using the wireless communication technology to form a network system that supports mutual communication and resource sharing. The essential feature of WLAN is to connect computers to the Internet in wireless mode rather than by using communication cables, facilitating network construction and terminal migration.

AP

Access Point (AP): AP is used for a wireless terminal to access the wired network. It serves as the communication bridge between a wireless terminal and wired network.

STA

Wireless user: A user who accesses the Internet by using a wireless terminal.

RSSI

Received Signal Strength Indication (RSSI) is used to indicate the quality of a wireless link.

Overview

Function and Feature	Description
Terminating Low-Rate Applications	Terminate low-rate applications by configuring the rate set.
Increasing the Beacon Frame Period Appropriately	Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.
Configuring Rate Limit for Wireless Users	Make limited network resources serve more users.
Improving the Anti-Interference Capability	When there is co-channel interference, decrease the RTS threshold appropriately to improve the anti-interference capability.
Improving the Capability of Competing for Channels	Adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
Reducing Weak-Signal Terminals	To control the network coverage of the AP and improve the transmission quality of wireless signals, limit the number of wireless access users.
Limiting the STA Access Number for an AP	Limit the STA number on the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.
Establishing a Pure 11n Network	Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.
Spectrum Navigation	Guide access of the dual-band STA to the 5G frequency band that has stronger access capacity by means of band selection to reduce the pressure of the 2.4G frequency band, thereby improving user experience.
One-Click Network Optimizaion	After the wireless network runs for a period of time, the following problems may occur: The network speed is slow. Signal or interference problems exist. The authentication page cannot be displayed. STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band. A large number of low-rate packets exist. Multicast packets are lost or re-transmitted. In this case, network optimization is required.

2.3.1 Terminating Low-Rate Applications

Working Principle

Terminate low-rate applications by configuring the rate set.

2.3.2 Increasing the Beacon Frame Period Appropriately

Working Principle

Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

2.3.3 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Working Principle

Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.

2.3.4 Configuring Rate Limit for Wireless Users

Working Principle

To make limited network resources serve more users, ensure that the device supports the traffic rate limit function. When the data traffic accords with the committed rate, data packets are allowed to pass. When the data traffic does not accord with the committed rate, data packets are discarded.

2.3.5 Improving the Anti-Interference Capability

Working Principle

To avoid data transmission failure caused by conflicts between channels, the IEEE 802.11 MAC protocol provides a Request to Send/Clear to Send (RTS/CTS) handshake protocol, that is, requests to send/allow sending protocol. The following description assumes that workstation A needs to send data to workstation B. First of all, workstation A sends a RTS request frame. If workstation B allows workstation A to send the request frame, workstation B replies a CTS permission frame. After receiving this permission frame, workstation A begins to sending data. If multiple workstations send RTS requests to the same workstation, only the workstations receiving CTS are allowed to send data. For the workstation not receiving CTS, it is regarded that channel conflict occurs. In this case, this workstation waits for a certain time and sends a RTS request again.

If RTS/CTS handshake needs to be performed when a workstation sends data each time, excessive RTS frames will occupy much channel bandwidth. Users can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with a length smaller than the RTS threshold.

2.3.6 Improving the Capability of Competing for Channels

Working Principle

EDCA parameters differentiate access capabilities of channels with different priorities. Each AC has its own EDCA channel competition parameters. Users can adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.

During actual configuration, you can choose to configure the EDCA parameters on the client or side based on application requirements. Configuration of EDCA parameters on the client and AP respectively affects the downlink data traffic and uplink data traffic.

2.3.7 Reducing Weak-Signal Terminals

Working Principle

Wireless users search for the AP in active scanning or passive scanning mode.

- Active scanning: A wireless user sends a Probe Request for accessing the AP. After confirming the request frame, the AP returns a Probe Response frame.
- Passive scanning: The AP periodically broadcasts Beacon frames. A wireless user attempts to connect to the AP after listening Beacon frames.

To control the network coverage of the AP and improve the transmission quality of wireless signals, limit the number of wireless access users. You can control the Beacon frame broadcast coverage of the AP to prevent access of remote wireless users. You can also limit the minimum value of the RSSI for wireless users. When the RSSI of the request frame sent from a wireless user is smaller than this minimum value, the access of this wireless user is not allowed.

2.3.8 Limiting the STA Number for an AP

Working Principle

In a WLAN, one AP allows access of multiple wireless users, and the administrator can specify the maximum number of wireless users. Limit the STA access number for the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.

2.3.9 Establishing a Pure 11n Network

Working Principle

Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.

2.3.10 Spectrum Navigation

Working Principle

IEEE802.11 mainly has two communication frequency bands:

- 2.4 GHz (2.412 to 2.4835 GHz) (IEEE 802.11b/g operates in this frequency range)
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz) (IEEE 802.11a operates in this frequency range)

Dual-band STA supports both 2.4G and 5G frequency bands. However, users lack professional knowledge; most wireless access service vendors do not provide effective guidance; 802.11b/g is more widely applied than 802.11a. Consequently, many dual-band STAs only use the 2.4G frequency band, causing congestion of the 2.4G frequency band and waste of the 5G frequency band. In fact, the 5G frequency band has a stronger access capacity than the 2.4G frequency band: The 2.4G frequency band at most has three non-overlapping communication channels, whereas the 5G frequency band can

provide more than three non-overlapping communication channels. For example, 13 in China and up to 24 in North America.

Guide access of the dual-band STA to the 5G frequency band that has stronger access capacity by means of band selection to reduce the pressure of the 2.4G frequency band, thereby improving user experience.

2.3.11 One-Click Network Optimization

Working Principle

After the wireless network runs for a period of time, the following problems may occur:
The network speed is slow.
Signal or interference problems exist.
The authentication page cannot be displayed.

STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band.
A large number of low-rate packets exist.
Multicast packets are lost or re-transmitted.
In this case, network optimization is required.

1. The network speed is slow.

The possible causes are as follows:
No rate limit is configured. Some users occupy large bandwidth for downloading or playing videos. As a result, the network speed of other users is slow.
A rate limit is configured but the rate is high, without achieving the rate limit effect.
A rate limit is configured but the rate is low, resulting in slow network speed.
For this problem, the rate limit solution can be used. Rate limiting is performed for all STAs by WLAN to ensure that the average uplink and downlink rate is 256 kbit/s and the abrupt rate is 300 kbit/s.

2. Signal or interference problems exist.

For example, the signal is poor, roaming frequently occurs, or intra-frequency/inter-frequency interference occurs. For this problem, the RRM function can be used. After the RRM function is enabled, channel or power adjustment is performed for online APs or newly added APs to ensure signal coverage and channel different from those of neighboring APs. If the poor signal or intra-frequency/inter-frequency interference problem does not exist, disable the RRM function to improve the device performance.

3. The authentication page cannot be displayed.

This is because few sessions are configured. For this problem, restore the default number of sessions to ensure that each STA supports 255 sessions and each port supports 1000 sessions by default.

4. STAs equipped with 2.4 GHz/5 GHz network cards are usually associated the network at the 2.4 GHz band.

For this problem, the 5 GHz preferred function can be used. If only few STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be disabled.

5. A large number of low-rate packets exist.

For this problem, the low-rate packet forbidding function can be used to forbid packets complying with 802.11b, 802.11g, or 802.11a and with a rate lower than 11 Mbps.

6. Multicast packets are lost or re-transmitted.

This is because a high multicast rate is set. For this problem, restore the default multicast rate to ensure user experience.

2.3.12 Intelligent Network Optimization

Perform wireless network optimization intelligently.

Working Principle

Perform wireless network optimization intelligently based on real-time network running.

2.3.13 Mcell Configuration

Enable dense deployment optimization.

Working Principle

Enable dense deployment optimization.

2.3.14 Roaming Stickiness

Working Principle

Monitor terminals with low RSSI and poor user experience on the entire wireless network in real time and determine whether more suitable APs exist for terminals to access the network based on the terminal detection information collected by each AP. If such terminals with sticky roaming exist, the AP sends a deauthentication frame to disassociate with the terminal to ensure that the terminal is associated with an AP with better signal quality.

2.3.15 Remote Association Information Collection

Working Principle

Determine whether a terminal is associated with the AP with the optimal signal quality based on the terminal detection information. If it is detected that a terminal associates with an AP with poor signal quality, a notification is reported to the WIS client. Based on collected remote association information, the WIS client performs coverage optimization for APs.

2.3.16 Automatic Device Information Upload

Working Principle

Configure automatic upload of the AC and AP software and hardware version numbers.

2.4 Configuration

Configuration Item	Configuration Suggestion & Relevant Command	
Configuring the Rate Set	⚠ Optional. It is used to terminate low-rate applications.	
	802.11a network rate	Configures the 11a rate set.
	802.11b network rate	Configures the 11b rate set.
	802.11g network rate	Configures the 11g rate set.

Configuring the Beacon Frame Period	Optional. It is used to increase the Beacon frame period.	
	beacon period	Configures the Beacon frame period.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	Optional. It is used to enable layer 2 isolation of wireless users in a VLAN.	
	user-isolation ssid_ap enable	Configures WLAN-based user isolation for an AP.
	user-isolation ap enable	Configures user isolation for an AP.
	user-isolation ssid_ac enable	Configures WLAN-based user isolation for an AC.
	user-isolation ac enable	Configures user isolation for an AC.
Configuring Rate Limit for Wireless Users	Optional. It is used to configure rate limit for wireless users.	
	ap-based	Configures AP-based rate limit.
	netuser	Configures client-based rate limit.
	wlan-based	Configures WLAN-based rate limit.
Configuring the RTS/CTS Protection Mechanism	Optional. It is used to configure the RTS/CTS protection mechanism.	
	rts-threshold	Configures the RTS threshold.
Configuring EDCA Parameters	Optional. It is used to configure EDCA parameters.	
	wmm edca-client	Configures the EDCA parameters on the client.
	wmm edca-radio	Configures the EDCA parameters on the AP.
Configuring the Allowed Access Signal Strength	Optional. It is used to configure the allowed access signal strength.	
	response-rssi	Configures the minimum RSSI for wireless user access.
	coverage-area-control	Configures the management frame transmit power.
Configuring the Number of Access Users Allowed by the AP	Optional. It is used to configure the number of access users allowed by the AP.	
	sta-limit	Configures AP-based STA number limit.
Configuring a Pure 11n Network	Optional. It is used to configure a pure 11n network.	
	11asupport	Configures whether to support 11a or not.
	11bsupport	Configures whether to support 11b or not.
	11gsupport	Configures whether to support 11g or not.
	11nasupport	Configures whether to support 11na or not.
	11ngsupport	Configures whether to support 11ng or not.
Configuring Spectrum Navigation	Mandatory. It is used to enable the spectrum navigation function of the WLAN.	
	band-select enable	Enables the spectrum navigation function.

	⚠ Optional. It is used to configure the operating parameters of the spectrum navigation function.	
	band-select acceptable-rssi	Configures the lower limit of STA signal strength accepted by spectrum navigation.
	band-select access-denial	Configures the number of times for which dual-band STA access to 2.4G band is denied.
	band-select age-out	Configures the STA information aging time.
	band-select probe-count	Configures the detection period count of suppression STA.
	band-select scan-cycle	Configures the threshold of STA detection scanning period.
Configuring One-Click Network Optimization	⚠ Optional. It is used to configure network optimization options.	
	wopt choose	Configures network optimization options.
	⚠ Optional. It is used to configure one-click network optimization.	
	wopt enable	Configures one-click network optimization.
Configuring Intelligent Network Optimization	⚠ Optional. It is used to configure network optimization options.	
	wis enable	Enables intelligent network optimization.
Configuring mcell	⚠ Optional. It is used to configure network optimization options.	
	mcell enable	Enables dense deployment optimization.
Configuring Roaming Stickness	⚠ Optional. It is used to configure network optimization options.	
	sticky-steering monitor-only	Enables roaming stickiness monitoring.
	⚠ Optional. It is used to configure one-click network optimization.	
	sticky-steering enable	Enables roaming stickiness navigation.
Configuring Remote Association	⚠ Optional. It is used to configure network optimization options.	
	farpoint-steering enable	Enables remote association.

2.4.1 Configuring the Rate Set

Configuration Effect

- Configure the rate set to terminate low-rate applications; prohibit packet transmission at low rate between the STA and AP; improve the channel usage.

Notes

- If you disable a rate, this rate can no longer be used.
- If you disable all rates, wireless users cannot access the WLAN.

- If you disable all 11b rates, 11b wireless users cannot access the WLAN.

Configuration Steps

Configuring the 11a Rate Set

- Mandatory configuration. By default, configuration of rates 6 Mbps, 12 Mbps, and 24 Mbps is mandatory, and configuration of rates 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring the 11b Rate Set

- Optional configuration. By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring the 11g Rate Set

- Optional Configuration. By default, configuration of rates 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps is mandatory, and configuration of rates 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps is optional.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of the rate set.

Related Commands

Configuring the 11a Rate Set

Command	**802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuring the 11b Rate Set

Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disable** | **mandatory** | **supported** }
Parameter	**1**: The rate is 1 Mbps.

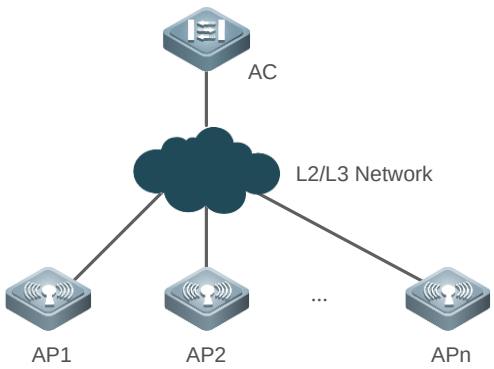
Description	**2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **11**: The rate is 11 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuring the 11g Rate Set

Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**1**: The rate is 1 Mbps. **2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **11**: The rate is 11 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	N/A
Usage Guide	N/A

Configuration Examples

Configuring the Rate Set

Scenario **Figure 2-3**	
Configuration Steps	● Disable the 6 Mbps rate for 802.11a users on the AC device. ● Disable the 1 Mbps and 2 Mbps rates for the 802.11b users on the AC device. ● Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g users on the AC device.
AC	Ruijie#configure terminal Ruijie(config)#ac-controller Ruijie(config-ac)#802.11a network rate 6 disabled Ruijie(config-ac)#802.11b network rate 1 disabled Ruijie(config-ac)#802.11b network rate 2 disabled Ruijie(config-ac)#802.11g network rate 1 disabled Ruijie(config-ac)#802.11g network rate 2 disabled Ruijie(config-ac)#802.11g network rate 5 disabled
Verification	After configuring the rate set, you can display the configuration information of the rate set for a check. ● You can run the **show running** command to display the configuration information of the rate set.
	Ruijie#show running ! ac-controller country CN country US 802.11g network rate 1 disabled 802.11g network rate 2 disabled 802.11g network rate 5 disabled 802.11g network rate 11 mandatory 802.11g network rate 6 supported 802.11g network rate 9 supported 802.11g network rate 12 supported 802.11g network rate 18 supported 802.11g network rate 24 supported 802.11g network rate 36 supported 802.11g network rate 48 supported 802.11g network rate 54 supported 802.11b network rate 1 disabled 802.11b network rate 2 disabled

```
802.11b network rate 5 mandatory
802.11b network rate 11 mandatory
802.11a network rate 6 disabled
802.11a network rate 9 supported
802.11a network rate 12 mandatory
802.11a network rate 18 supported
802.11a network rate 24 mandatory
802.11a network rate 36 supported
802.11a network rate 48 supported
802.11a network rate 54 supported
!
```

Common Errors

None.

2.4.2 Configuring the Beacon Frame Period

Configuration Effect

- Lengthen the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

Notes

- If Beacon frame period is set to too great, users may get disconnected from the WLAN or detect the WLAN frequently.

Configuration Steps

Configuring the Beacon Frame Period

- Optional configuration. By default, the Beacon frame period is 100 milliseconds.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the Beacon frame period.

Related Commands

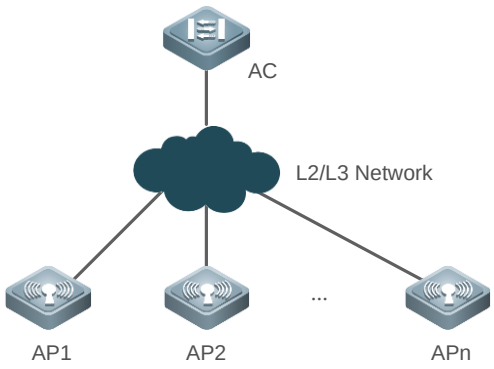
Configuring the Beacon Frame Period

Command	**beacon period** *milliseconds* **radio** *radio-id*
Parameter Description	*milliseconds*: Specifies the Beacon frame period, in the range from 20 to 1,000 in the unit of milliseconds. *radio-id*: Specifies the RF interface index, in the range from 1 to 48.
Command Mode	AP configuration mode

Defaults	100 milliseconds
Usage Guide	Configuration for all APs is not supported.

Configuration Examples

Configuring the Beacon Frame Period

Scenario **Figure 2-4**	
Configuration Steps	● Set the Beacon frame period of AP1 Radio1 to 300 milliseconds on the AC device.
AC	Ruijie#configure terminal Ruijie(config)#ap-config AP1 Ruijie(config-ap)#beacon period 300 radio 1
Verification	After configuring the Beacon frame period, you can display the configuration information of the Beacon frame period for a check. ● You can run the **show ap-config running** command to display the configuration information of the Beacon frame period.
	Ruijie#show ap-config running AP1 ! ap-config AP1 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1

	no enable-radio 2 !

Common Errors

None.

2.4.3 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Configuration Effect

- Configure this function for the network not requiring layer 2 mutual-access to decrease network attacks and multicast packet bandwidth usage.

Notes

- None.

Configuration Steps

Configuring WLAN-Based User Isolation for an AP

- Optional configuration. By default, WLAN-based user isolation is disabled for the AP.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring User Isolation for an AP

- Optional configuration. By default, user isolation is disabled for the AP.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring WLAN-Based User Isolation for an AC

- Optional configuration. By default, WLAN-based user isolation is disabled for the AC.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Configuring User Isolation for an AC

- Optional configuration. By default, user isolation is disabled for the AC.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of layer 2 isolation of wireless users in a VLAN.

Related Commands

Configuring WLAN-Based User Isolation for an AP

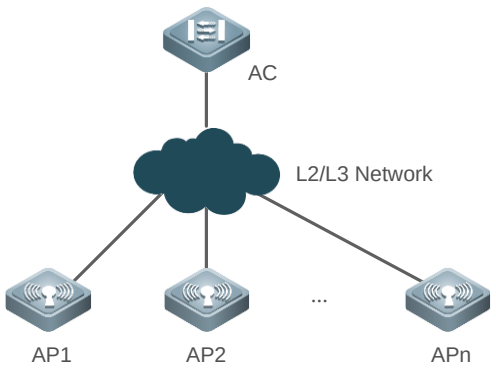
Configuring User Isolation for an AP

Configuring WLAN-Based User Isolation for an AC

Configuring User Isolation for an AC

Configuration Examples

Configuring Layer 2 Isolation of Wireless Users in a VLAN

Scenario **Figure 2-5**	
Configuration Steps	● Enable WLAN-based user isolation for an AP on the AC device. ● Enable user isolation for an AP on the AC device. ● Enable WLAN-based user isolation for an AC on the AC device. ● Enable user isolation for an AC on the AC device.
AC	`Ruijie#configure terminal` `Ruijie(config)#wids` `Ruijie(config-wids)#user-isolation ssid-ap enable` `Ruijie(config-wids)#user-isolation ap enable` `Ruijie(config-wids)#user-isolation ssid-ac enable` `Ruijie(config-wids)#user-isolation ac enable`
Verification	After configuring layer 2 isolation of wireless users in a VLAN, you can display the configuration information on layer 2 isolation of wireless users in a VLAN for a check. ● You can run the **show running** command to display the configuration information on layer 2 isolation of wireless users in a VLAN.
	`Ruijie#show running` `!` `wids` ` user-isolation ap enable` ` user-isolation ac enable` ` user-isolation ssid-ac enable` ` user-isolation ssid-ap enable` `!`

2.4.4 Configuring Rate Limit for Wireless Users

Configuration Effect

- To make limited network resources serve more users, ensure that the device supports the traffic rate limit function. When the data traffic accords with the committed rate, data packets are allowed to pass. When the data traffic does not accord with the committed rate, data packets are discarded.

Notes

- When the data traffic does not accord with the committed rate, data packets are discarded.

Configuration Steps

Configuring AP-Based Rate Limit

- Optional configuration. By default, AP-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Configuring Client-Based Rate Limit

- Optional configuration. By default, client-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in AC configuration mode on the AC device.

Configuring WLAN-Based Rate Limit

- Optional configuration. By default, WLAN-based rate limit is disabled.
- Unless otherwise specified, the configuration shall be performed in WLAN configuration mode on the AC device.

Verification

- You can run the **show running** command to display the configuration information of the rate limit for wireless users.

Related Commands

Configuring AP-Based Rate Limit

Command	**ap-based { per-user-limit | total-user-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users on the AP. **total-user-limit**: Limits the rate of the whole AP is limited. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of . *burst-data-rate*: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .
Command Mode	AP configuration mode
Defaults	AP-based rate limit is disabled by default.
Usage Guide	N/A

Configuring Client-Based Rate Limit

Command	**netuser** *mac-address* **{ inbound | outbound } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: Specifies the MAC address of the user. **inbound**: Limits the rate of uplink traffic. **outbound**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of .

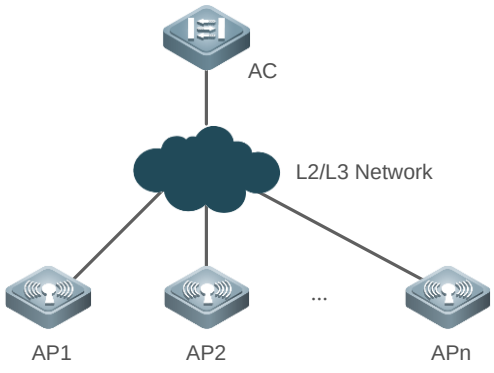
	burst-data-rate: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .
Command Mode	AC configuration mode
Defaults	Client-based rate limit is disabled by default.
Usage Guide	N/A

Configuring WLAN-Based Rate Limit

Command	**wlan-based { per-user-limit | total-user-limit | per-ap-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users in the WLAN. **total-user-limit**: Limits the rate of the whole WLAN. **per-ap-limit**: Limits the rate of the whole WLAN for each AP separately. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the range from 8 to 261120 in the unit of . *burst-data-rate*: Specifies the burst rate limit, in the range from 8 to 261120 in the unit of .
Command Mode	WLAN configuration mode
Defaults	WLAN-based rate limit is disabled by default.
Usage Guide	N/A

Configuration Examples

Configuring Rate Limit for Wireless Users

Scenario Figure 2-6	
Configuration Steps	● Limit the maximum uplink average rate and maximum uplink burst rate of each user on AP1 to 256*8 Kbps and 1024*8 Kbps respectively on the AC device. ● Limit the maximum uplink average rate and maximum uplink burst rate of wireless user 14cf.920b.bfce on the AC to 256* 8 Kbps and 1024*8 Kbps respectively on the AC device. ● Limit the maximum uplink average rate and maximum uplink burst rate of each user in WLAN 12 to 256*8 Kbps and 1024*8 Kbps respectively on the AC device.
	`Ruijie#configure terminal` `Ruijie(config)#ap-config AP1` `Ruijie(config-ap)#ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate`

	1024 Ruijie(config-ap)#end Ruijie#configure terminal Ruijie(config)#ac-controller Ruijie(config-ac)#netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024 Ruijie(config-ap)#end Ruijie#configure terminal Ruijie(config)#wlan-config 12 Ruijie(config-wlan)#wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
Verification	After configuring the rate limit for wireless users, you can display the configuration information of the rate limit for wireless users for a check. ● You can run the **show running** command to display the configuration information of the rate limit for wireless users.
	Ruijie#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 ! Ruijie#show running ! wlan-config 12 wlan_opt wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 enable-broad-ssid ! ! ac-controller netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024

```
country CN
country US
802.11g network rate 1 disabled
802.11g network rate 2 disabled
802.11g network rate 5 disabled
802.11g network rate 11 mandatory
802.11g network rate 6 supported
802.11g network rate 9 supported
802.11g network rate 12 supported
802.11g network rate 18 supported
802.11g network rate 24 supported
802.11g network rate 36 supported
802.11g network rate 48 supported
802.11g network rate 54 supported
802.11b network rate 1 disabled
802.11b network rate 2 disabled
802.11b network rate 5 mandatory
802.11b network rate 11 mandatory
802.11a network rate 6 disabled
802.11a network rate 9 supported
802.11a network rate 12 mandatory
802.11a network rate 18 supported
802.11a network rate 24 mandatory
802.11a network rate 36 supported
802.11a network rate 48 supported
802.11a network rate 54 supported
!
```

Common Errors

None.

2.4.5 Configuring the RTS/CTS Protection Mechanism

Configuration Effect

- When co-channel interference exists, a smaller RTS threshold means a higher anti-interference capability. However, more RTS/CTS packets require higher channel usage for packet control, reducing the available channel bandwidth for wireless users. Users can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with a length smaller than the RTS threshold.

Notes

- None.

Configuration Steps

↘ Configuring the RTS Threshold

- Optional configuration. By default, the RTS threshold is 2347 bytes.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the RTS threshold.

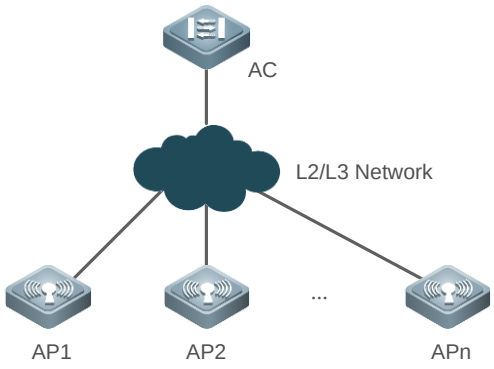
Related Commands

Configuring the RTS Threshold

Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: Specifies the RTS threshold, in the range from 257 to 2,347 in the unit of bytes. *radio-id*: Specifies the RF interface index, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	The RTS threshold is 2,347 bytes by default.
Usage Guide	N/A

Configuration Examples

Configuring the RTS Threshold

Scenario Figure 2-7	
Configuration Steps	● Set the RTS threshold of AP1 Radio1 to 800 bytes on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)#ap-config AP1` `Ruijie(config-ap)#rts-threshold 800 radio 1`
Verification	After configuring the RTS threshold, you can display the configuration information of the RTS threshold for a check. ● You can run the **show ap-config running** command to display the configuration information of the RTS threshold.
	`Ruijie#show ap-config running AP1` `!` `ap-config AP1`

```
ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
no 11acsupport enable radio 1
no 11acsupport enable radio 2
802.11n mcs support 15 radio 1
802.11n mcs support 15 radio 2
rts-threshold 800 radio 1
antenna receive 3 radio 1
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

Common Errors

None.

2.4.6 Configuring EDCA Parameters

Configuration Effect

- During actual configuration, you can choose to configure the EDCA parameters on the client or AP based on application requirements. Configuration of EDCA parameters on the client and AP respectively affects the downlink data traffic and uplink data traffic.

Notes

- None.

Configuration Steps

Configuring the EDCA Parameters on the Client

- Optional configuration. By default, the EDCA parameters on the client are as follows:
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Configuring the EDCA Parameters on the AP

- Optional configuration. By default, the EDCA parameters on the AP are as follows:
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the EDCA parameters.

Related Commands

Configuring the EDCA Parameters on the Client Side

Command	**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the aifsn value, in the range from 1 to 15. *cwmin-value*: Sets the cwmin value, in the range from 0 to 15. *cwmax-value*: Sets the cwmax value, in the range from 0 to 15. *txop-value*: Sets the txop value, in the range from 0 to 255 in the unit of 32 microseconds. *queue-length*: Sets the AC queue length, in the range from 1 to 768. The default is 768. *radio-id*: Sets the EDCA parameters on the client, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	AC / AIFS / CWmin / CWmax / TXOP back-ground / 7 / 4 / 10 / 0 best-effort / 3 / 4 / 10 / 0 video / 2 / 3 / 4 / 94 voice / 2 / 2 / 3 / 47
Usage Guide	The parameter configuration takes effect only when the wmm service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a message indicating configuration failure is displayed.

Configuring the EDCA Parameters on the AP Side

Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the aifsn value, in the range from 1 to 15. *cwmin-value*: Sets the cwmin value, in the range from 0 to 15. *cwmax-value*: Indicates setting of the cwmax value, in the range from 0 to 15. *txop-value*: Sets the txop value, in the range from 0 to 255 in the unit of 32 microseconds. **noack**: Enables the no ack policy. The no ack policy is not enabled by default. *radio-id*: Sets radio of the EDCA parameters on the client, in the range from 1 to 48.
Command	AP configuration mode

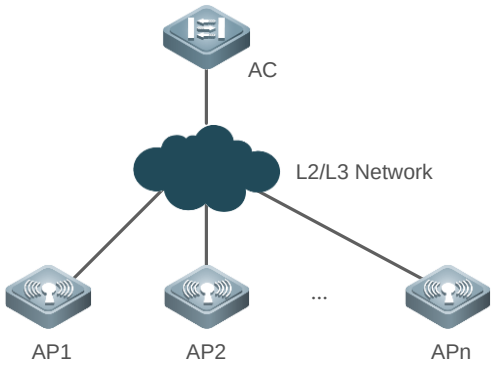
Mode	
Defaults	

AC	AIFS	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

Usage Guide	The parameter configuration takes effect only when the wmm service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a message indicating configuration failure is displayed.

Configuration Examples

Configuring EDCA Parameters

Scenario Figure 2-8	
Configuration Steps	● Configure the EDCA parameters on the client of AP1 Radio1 on the AC. ● Configure the EDCA parameters on the AP of AP1 Radio1 on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)#ap-config AP1` `Ruijie(config-ap)#wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1` `Ruijie(config-ap)#wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1`
Verification	After configuring the EDCA parameters, you can display the configuration information of the EDCA parameters for a check. ● You can run the **show ap-config running** command to display the configuration information of the EDCA parameters.
	`Ruijie#show ap-config running AP1` `!` `ap-config AP1` ` wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1` ` wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1` ` no 11acsupport enable radio 1` ` no 11acsupport enable radio 2`

```
802.11n mcs support 15 radio 1
802.11n mcs support 15 radio 2
antenna receive 3 radio 1
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

Common Errors

None.

2.4.7 Configuring the Allowed Access Signal Strength

Configuration Effect

- You can control the Beacon frame broadcast coverage of the AP to prevent access of remote wireless users. You can also limit the minimum value of the RSSI for wireless users. When the RSSI of the request frame sent from a wireless user is smaller than this minimum value, the access of this wireless user is prohibited.

Notes

- If the minimum RSSI for wireless user access is set to too great, many wireless users may fail to access the WLAN.
- If the management frame transmit power is set to too great, many remote wireless users may fail to discover the network.

Configuration Steps

↘ Configuring the Minimum RSSI for Wireless User Access

- Optional configuration. By default, the minimum RSSI for wireless user access is 0. That is, all users are allowed to access the WLAN, no matter how large the RSSI is.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

↘ Configuring the Management Frame Transmit Power

- Optional configuration. By default, the management frame transmit power is 0. That is, the management frame transmit power is not configured by default.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC.

Verification

- You can run the **show ap-config running** command to display the configuration information of the allowed access signal strength.

Related Commands

Configuring the Minimum RSSI for Wireless User Access

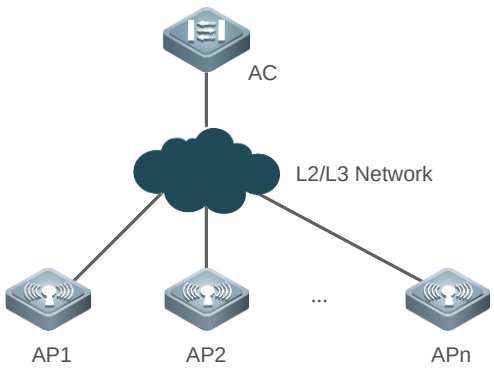
Command	**response-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi*: Specifies the minimum RSSI for wireless user access, in the range from 0 to 100 in the unit of dB. *radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	The default RSSI is 0.
Usage Guide	N/A

Configuring the Management Frame Transmit Power

Command	**coverage-area-control** *power* **radio** *radio-id*
Parameter Description	*power*: Specifies the management frame transmit power, in the range from 0 to32 in the unit of dBm. *radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	The default power is 0.
Usage Guide	N/A

Configuration Examples

Configuring the Allowed Access Signal Strength

Scenario **Figure 2-9**	
Verification	● Set the minimum RSSI for wireless user access of AP1 Radio1 to 20 dB on the AC. ● Set the management frame transmit power of AP1 Radio1 to 30 dBm on the AC.

AC	Ruijie#configure terminal Ruijie(config)#ap-config AP1 Ruijie(config-ap)#response-rssi 20 radio 1 Ruijie(config-ap)#coverage-area-control 30
Configuration Steps	After configuring the allowed access signal strength, you can display the configuration information of the allowed access signal strength for a check. ● You can run the **show ap-config running** command to display the configuration information of the allowed access signal strength.
	Ruijie#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 rts-threshold 800 radio 1 coverage-area-control 30 response-rssi 20 radio 1 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 !

Common Errors

None.

2.4.8 Configuring the Number of Access Users Allowed by the AP

Configuration Effect

- Limit the STA number for the AP to implement load balancing to a certain extent, avoiding uneven distribution of AP access users.

Notes

- None.

Configuration Steps

Configuring AP-Based STA Number Limit

- Optional configuration. By default, the AP-based STA number limit is 32.
- Unless otherwise specified, the configuration shall be performed in AP configuration mode on the AC device.

Verification

- You can run the **show ap-config running** command to display the configuration information of the AP-based STA number limit.

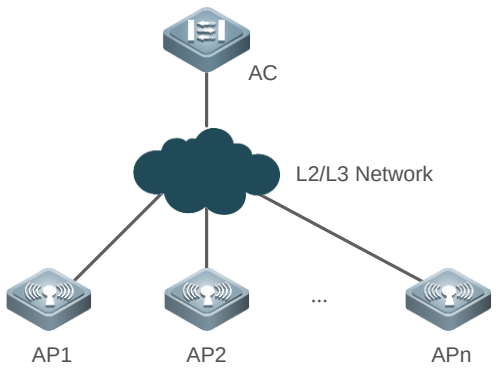
Related Commands

Configuring AP-Based STA Number Limit

Command	**sta-limit** *max-num*
Parameter Description	*max-num*: Specifies the AP-based STA number limit, in the range from 1 to 32.
Command Mode	AP configuration mode
Defaults	The default limit is 32.
Usage Guide	N/A

Configuration Examples

Configuring AP-Based STA Number Limit

Scenario Figure 2-10	
Configuration Steps	● Set the number of access users allowed by AP1 to 12 on the AC.
AC	Ruijie#configure terminal Ruijie(config)#ap-config AP1 Ruijie(config-ap)#sta-limit 12

Verification	After configuring the number of access users allowed by the AP, you can display the configuration information of the number of access users allowed by the AP for a check. ● You can run the **show ap-config running** command to display the configuration information of the number of access users allowed by the AP.
	Ruijie#show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1 802.11n mcs support 15 radio 2 rts-threshold 800 radio 1 coverage-area-control 30 response-rssi 20 radio 1 antenna receive 3 radio 1 antenna receive 3 radio 2 antenna transmit 3 radio 1 antenna transmit 3 radio 2 radio-type 1 802.11b radio-type 2 802.11a sta-limit 12 beacon period 300 radio 1 beacon period 100 radio 2 ap-mac 001a.a9c5.3f49 no enable-radio 1 no enable-radio 2 !

Common Errors

None.

2.4.9 Configuring a Pure 11n Network

Configuration Effect

- Configure a pure 11n network to prohibit access of non-11n devices; make all the 11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.

Notes

- Pure 11n network does not allow access of non-11n devices.

Configuration Steps

↘ Configuring Whether to Support 11a or Not

- Optional configuration. By default, access of 11a users at 5 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Configuring Whether to Support 11b or Not

- Optional configuration. By default, access of 11b users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Configuring Whether to Support 11g or Not

- Optional configuration. By default, access of 11g users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Configuring Whether to Support 11na or Not

- Optional configuration. By default, access of 11n users at 5 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Configuring Whether to Support 11ng or Not

- Optional configuration. By default, access of 11n users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Verification

- You can run the **show ap-config running** command to display the configuration information of the pure 11n network.

Related Commands

Configuring Whether to Support 11a or Not

Command	**11asupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	802.11a is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11b or Not

Command	**11bsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.

Command Mode	AP configuration mode
Defaults	802.11b is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11g or Not

Command	**11gsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	802.11g is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11na or Not

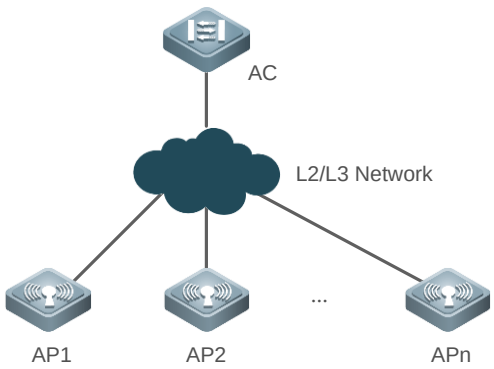
Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	802.11n at 5GHz is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. Configuration for all APs is not supported.

Configuring Whether to Support 11ng or Not

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of the radio to be configured, in the range from 1 to 48.
Command Mode	AP configuration mode
Defaults	802.11n at 2.4GHz is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. Configuration for all APs is not supported.

Configuration Examples

Configuring a Pure 11n Network

Scenario **Figure 2-11**	 ● AP1 Radio1 operates at 2.4 GHz. ● AP1 Radio2 operates at 5.8 GHz.
Configuration Steps	● Configure AP1 Radio1 as a pure 11n network on the AC device. ● Configure AP1 Radio2 as a pure 11n network on the AC device.
AC	`Ruijie#configure terminal` `Ruijie(config)#ap-config AP1` `Ruijie(config-ap)#no 11bsupport enable radio 1` `Ruijie(config-ap)#no 11gsupport enable radio 1` `Ruijie(config-ap)#11ngsupport enable radio 1` `Ruijie(config-ap)#no 11asupport enable radio 2` `Ruijie(config-ap)#11nasupport enable radio 2`
Verification	After configuring a pure 11n network, you can display the configuration information of the pure 11n network for a check. ● You can run the **show ap-config running** command to display the configuration information of the pure 11n network.
	`Ruijie#show ap-config running AP1` `!` `ap-config AP1` ` ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024` ` no 11asupport enable radio 2` ` no 11bsupport enable radio 1` ` no 11gsupport enable radio 1` ` no 11acsupport enable radio 1` ` no 11acsupport enable radio 2` ` 802.11n mcs support 15 radio 1` ` 802.11n mcs support 15 radio 2` ` rts-threshold 800 radio 1` ` coverage-area-control 30` ` response-rssi 20 radio 1`

```
antenna receive 3 radio 1
antenna receive 3 radio 2
antenna transmit 3 radio 1
antenna transmit 3 radio 2
radio-type 1 802.11b
radio-type 2 802.11a
sta-limit 12
beacon period 300 radio 1
beacon period 100 radio 2
ap-mac 001a.a9c5.3f49
no enable-radio 1
no enable-radio 2
!
```

2.4.10 Configuring Spectrum Navigation

Configuration Effect

- The spectrum navigation function of the WLAN is enabled, guiding access of the dual-band STA to the 5G frequency band.

Configuration Steps

Enabling the Spectrum Navigation Function of the WLAN

- Mandatory configuration.
- Unless otherwise specified, this configuration shall be performed on the AC or fat AP.

Configuring the Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

- Optional configuration. This configuration is performed when the spectrum navigation coverage needs to be adjusted.
- Unless otherwise specified, this configuration shall be performed on the AC.

Configuring the Number of Times for Which Dual-Band STA Access to 2.4G Band is Denied

- Optional configuration. This configuration is performed when dual-band STA access to 2.4G band needs to be denied. If access of many dual-band STAs lasts for a very long time or fails after the configuration, you need to set a lower value or remove the configuration.
- Unless otherwise specified, this configuration shall be performed on the AC.

Configuring the STA Information Aging Time

- Optional configuration. If no dual-band STA switches to a single-band 2.4G STA in the environment, you can configure a relatively large aging time. Otherwise, you can configure a relatively small aging time. If you cannot determine whether this type of switching occurs in the environment, use the default configuration.
- Unless otherwise specified, this configuration shall be performed on the AC.

Configuring the Detection Period Count of Suppression STA

- Optional configuration. If a single-band 2.4G STA cannot discover the WLAN for a long time, you shall decrease the value.
- Unless otherwise specified, this configuration shall be performed on the AC.

Configuring the Threshold of STA Detection Scanning Period

- Optional configuration. If a single-band 2.4G STA cannot discover the WLAN for a long time, you shall decrease the value. It is recommended to use the default setting if the condition is unclear.
- Unless otherwise specified, this configuration shall be performed on the AC.

Verification

- Run the **show band-select configuration** command to display the spectrum navigation parameter configuration on the device.
- Run the **show running-config** command to display whether the spectrum navigation function is enabled for the WLAN.
- After the device operates for a certain time, run the **show band-select statistics** command to display the running statistics on the device.
- Capture packets to check whether spectrum navigation has controlled the active detection process.

Related Commands

Enabling the Spectrum Navigation Function of the WLAN

Command	**band-select enable**
Parameter Description	N/A
Command Mode	WLAN configuration mode
Defaults	Spectrum navigation is disabled by default.
Usage Guide	N/A

Configuring the Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Lower limit of STA RSSI accepted by spectrum navigation, in the range from -100 to -50 in the unit of dBm.
Command Mode	Global configuration mode
Defaults	The lower limit of STA RSSI accepted by spectrum navigation is -80 dBm.
Usage Guide	N/A

Configuring the Number of Times for Which Dual-Band STA Access to 2.4G Band is Denied

Command	**band-select access-denial** *value*
Parameter Description	*value*: Number of times for which dual-band STA access to 2.4G band is denied, in the range from 0 to 10.
Command Mode	Global configuration mode
Defaults	0
Usage Guide	N/A

Configuring the STA Information Aging Time

Command	**band-select age-out** { **dual-band** *value* **| suppression** *value* }
Parameter Description	**dual-band** *value*: Aging time of dual-band STA information, in the range from 20 to 120 in the unit of seconds. **suppression** *value*: Aging time of dual-band STA information, in the range from 10 to 60 in the unit of seconds.
Command Mode	Global configuration mode
Defaults	**dual-band** *value:* 60 seconds **suppression** *value:* 20 seconds
Usage Guide	It is recommended that the aging time of dual-band STA information be set to twice to three times as much as the aging time of suppression STA information.

Configuring the Detection Period Count Value of Suppression STA

Command	**band-select probe-count** *value*
Parameter Description	*value*: Detection period count of suppression STA, in the range from 1 to 10.
Command Mode	Global configuration mode
Defaults	2
Usage Guide	N/A

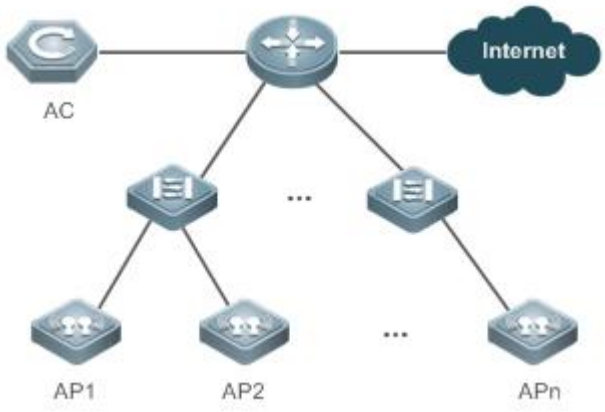
Configuring the Threshold of STA Detection Scanning Period

Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Threshold of STA detection scanning period, in the range from 1 to 1000 in the unit of milliseconds.

Command Mode	Global configuration mode
Defaults	200
Usage Guide	N/A

Configuration Examples

↘ Configuring WLAN Spectrum Navigation for Fit AP Architecture

Scenario Figure 2-12	 The preceding figure shows a wireless network of typical fit AP architecture. ● AC represents a wireless access controller. ● AP1, AP2… and AP*n* are all dual-band APs. ● The AC and APs are connected by layer 2 switching device and layer 3 routing device. ● To configure spectrum navigation WLAN as WLAN 99 with SSID "wlan-bandselect", map the WLAN to the two RF interfaces to all dual-band APs.
Configuration Steps	● Configure spectrum navigation parameters on the AC (optional). ● Enable the spectrum navigation function of WLAN 99 on the AC.
AC	`AC# configure terminal` `AC(config)# wlan-config 99` `AC(config-wlan)# band-select enable`
Verification	Use a dual-band STA to access WLAN "wlan-bandselect". ● Make the STA access the 5G frequency band. (The navigation may fail, and the STA may access the 2.4G frequency band.) ● Display the running statistics of spectrum navigation on the AC, and verify that the count increases.
AC	`A# show band-select statistics` `Band Select Statistics` `  Number of dual band client.............................. 1` `  Number of dual band client added.......................... 1`

	Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0

Common Errors

- Spectrum navigation parameters are improperly configured.
- The spectrum navigation function is not enabled.
- One of the two RF interfaces of the dual-band AP is disabled.

2.4.11 Configuring One-Click Network Optimization

Configuration Effect

- Improve the network performance.

Configuration Steps

Configuring Network Optimization Options

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt choose** command to configure network optimization options. At least one option is selected.
- Network optimization options can be configured via the network optimization function to improve network performance. Users can select network optimization options based on recommended configurations and actual network conditions. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, modify the configurations in corresponding mode.

Command	**wopt choose** { **band-select-disable** | **band-select-enable** | **low-rate-disable** | **multicast-speed** | **rrm-disable** | **rrm-enable** | **session-limit** | **speed-limit** }
Parameter Description	**band-select-disable**: Disables the 5 GHz preferred function. If only few STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be disabled. **band-select-enable**: Enables the 5 GHz preferred function. If a large number of STAs supporting 5 GHz exist in the environment, it is recommended that the 5 GHz preferred function be enabled. **low-rate-disable**: Forbids low-rate packets. Packets with a rate lower than 11 Mbps are forbidden. **multicast-speed**: Restores the default multicast rate (24 Mbps). **rrm-disable**: Disables the RRM function. If no intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be disabled. **rrm-enable**: Enables the RRM function. If intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be enabled to perform channel or power adjustment. **session-limit**: Restores the default number of sessions. The number of sessions affects authentication page pushing by iPortal. It is recommended that the default number of sessions be used. The default number of sessions is 255 for each STA and 1000 for each port. **speed-limit**: Limits the rate. (Rate limiting is performed for all STAs by WLAN. The average uplink and

	downlink rate is 256 kbit/s and the abrupt rate is 300 kbit/s.)
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Select network optimization options based on environment requirements. Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when selecting network optimization options. If incorrect configurations are optimized, modify the configurations in corresponding configuration mode manually.

Configuring One-Click Network Optimization

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt enable** command to configure one-click network optimization.
- One-click network optimization can be configured via the network optimization function to improve network performance. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, modify the configurations in corresponding mode.

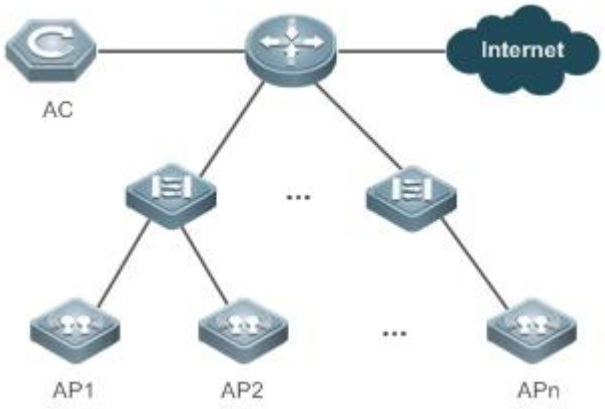
Command	**wopt enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	One-click network optimization can be configured if it is required to forbid low-rate packets, restore default multicast rates for WLANs, restore the default number of sessions, and limit rates for WLANs (average uplink and downlink rate is 256 kbit/s and abrupt rate is 300 kbit/s) in an actual environment. Note: Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when configuring one-click network optimization. If incorrect configurations are optimized, modify the configurations in corresponding configuration mode manually.

Verification

- Run the **show wopt** command to display network optimization information.

Configuration Example

Configuring Network Optimization Options in a Fit AP Architecture

Scenario **Figure 2-13**	 The preceding figure shows a typical wireless network with the fit AP architecture. ● AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs. ● The AC and AP are connected through a layer-2 switch and layer-3 router. ● Many STAs supporting 5 GHz exist in the environment. Therefore, it is recommended that the 5 GHz preferred function be enabled, that is, the spectrum navigation function be enabled. ● Low-rate packets are forbidden.
Configuration Steps	● Configure network optimization options on the AC.
AC	AC# configure terminal AC(config)# wopt choose band-select-enable low-rate-disable
Verification	After the user configures network optimization options, display the network optimization information for verification. ● Run the **show wopt** command to display network optimization information.
AC	AC# show wopt Low rate status: 802.11b rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 11 Mbps: Enable 802.11g rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 6 Mbps: Disable 9 Mbps: Disable 11 Mbps: Enable 802.11a rate:

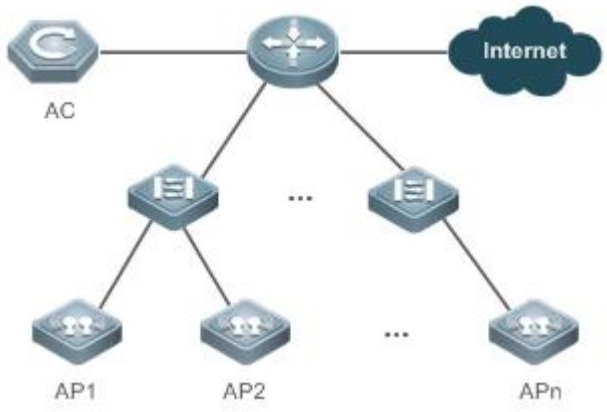
```
    6 Mbps: Disable
    9 Mbps: Disable

Multicast rate:
1    24  Mbps
2    24  Mbps
3    24  Mbps
4    24  Mbps
5    24  Mbps
6    24  Mbps
7    24  Mbps
8    24  Mbps
11   24  Mbps
12   24  Mbps
13   24  Mbps
14   24  Mbps
15   24  Mbps
16   24  Mbps
17   24  Mbps
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
```

```
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[6   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[7   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[8   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[11  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[12  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[13  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[14  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[15  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[16  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[17  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[18  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[19  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[100 ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
```

	wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]

Configuring One-Click Network Optimization in Fit AP Architecture

Scenario **Figure 2-14**	 The preceding figure shows a typical wireless network with the fit AP architecture. ● AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs. ● The AC and AP are connected through a layer-2 switch and layer-3 router. ● One-click network optimization is to be configured.
Configuration Steps	● Configure one-click network optimization on the AC.
AC	AC# configure terminal AC(config)# wopt choose band-select-enable low-rate-disable
Verification	After one-click network optimization is configured, display the network optimization information for verification. ● Run the **show wopt** command to display network optimization information.
AC	AC# show wopt Low rate status: 802.11b rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 11 Mbps: Enable 802.11g rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable

```
    6 Mbps: Disable
    9 Mbps: Disable
   11 Mbps: Enable
 802.11a rate:
    6 Mbps: Disable
    9 Mbps: Disable

Multicast rate:
1    24  Mbps
2    24  Mbps
3    24  Mbps
4    24  Mbps
5    24  Mbps
6    24  Mbps
7    24  Mbps
8    24  Mbps
11   24  Mbps
12   24  Mbps
13   24  Mbps
14   24  Mbps
15   24  Mbps
16   24  Mbps
17   24  Mbps
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.
```

```
wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest to enable RRM.

Speed limit:
 wlan[1   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[6   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[7   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[8   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[11  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[12  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[13  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[14  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[15  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[16  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[17  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
 wlan[18  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst:
300 Kbps]
```

	wlan[19] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[100] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]

2.4.12 Configuring Intelligent Network Optimization

Configuration Effect

- Perform intelligent network optimization based on network conditions.

Configuration Steps

- Run the **wis enable** command in configuration mode.

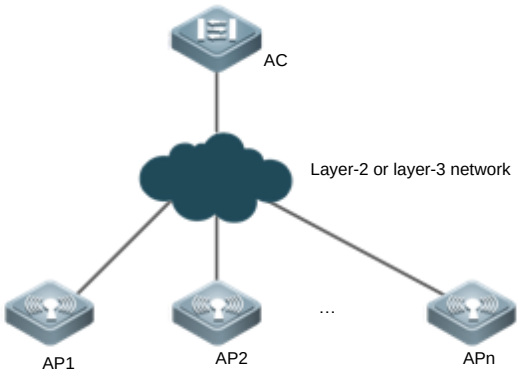
Command	**wis enable**
Parameter Description	N/A
Defaults	Intelligent network optimization is not configured by default.
Command Mode	AC global configuration mode
Usage Guide	After this command is run on a running network, intelligent optimization can be performed for the network. In normal cases, this command is used by network management personnel.

Verification

- Run the **show running** command to display the configurations.

Configuration Example

Configuring Intelligent Network Optimization

Scenario **Figure 2-15**	

Configuration Steps	● Enable intelligent network optimization on the AC.
AC	Ruijie#configure terminal Ruijie(config-ac)#wis enable
Verification	After intelligent network optimization is configured, display the configurations for verification. ● Run the **show running** command to display information about intelligent network optimization.
	Ruijie#show running ! wis enable !

2.4.13 Configuring Mcell

Configuration Effect

- Enable dense deployment optimization.

Configuration Steps

- Run the **mcell** command in AP configuration mode.

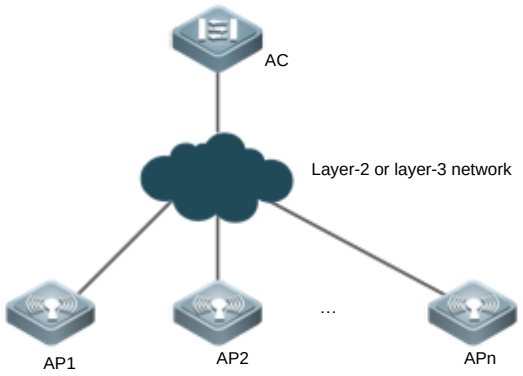
Command	mcell enable **radio** *radio-id*
Parameter Description	*radio-id*: Indicates the index of an RF port. The value range is 1 to 48.
Defaults	Mcell is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the configurations.

Configuration Example

↘ Configuring Mcell

Scenario **Figure 2-16**	
Configuration Steps	● Enable the Mcell function on the AC.
AC	Ruijie#configure terminal Ruijie(config)#ap-config AP1 Ruijie(config-ap)# mcell enable radio 1
Verification	After the Mcell function is configured, display the configurations for verification. ● Run the **show running** command to display information about the Mcell function.
	Ruijie#show ap-config running ap-config AP1 mcell enable radio 1

2.4.14 Configuring Roaming Stickiness

Configuration Effect

- Configure this function to enable roaming stickiness monitoring or navigation.

Notes

- The WIS must be enabled.

Configuration Steps

- Configure roaming stickiness in ap-config all or ap-group configuration mode.

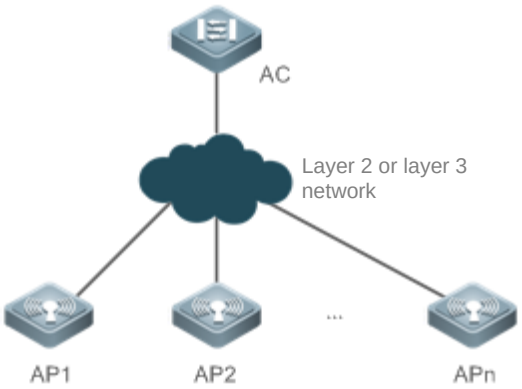
Command	**sticky-steering** { **monitor-only** | **enable** }
Parameter Description	**monitor-only**: Indicates the monitoring mode, that is, only roaming stickiness is monitored. **enable**: Indicates the navigation mode, that is, roaming stickiness navigation is performed if roaming stickiness is detected.
Defaults	By default, roaming stickiness is disabled.
Command Mode	Configure roaming stickiness for all AP groups in ap-config all mode, and configure roaming stickiness for a single AP group in ap-group mode.
Usage Guide	N/A

Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

Configuring Roaming Stickiness

Scenario **Figure 2-17**	
Configuration Steps	• Configure roaming stickiness monitoring on the AC. • Configure roaming stickiness navigation on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)#ap-config all` `Ruijie(config-ap)# sticky-steering monitor-only` `Ruijie(config-ap)# ap-group test1` `Ruijie(config-group)#sticky-steering enable`
Verification	• Run **show running** to query the roaming stickiness configuration information.
	`Ruijie#show running-config` `ap-group test1` ` sticky-steering enable` `!` `ap-group test2` ` sticky-steering monitor-only` `!` `ap-group test3` ` sticky-steering monitor-only` `!`

2.4.15 Configuring Remote Association Information Collection

Configuration Effect

- Enable remote association information collection to enable the WIS client to provide remote association optimization solutions.

Notes

- The WIS must be enabled.

Configuration Steps

- Enable remote association information collection in ap-config all or ap-group configuration mode.

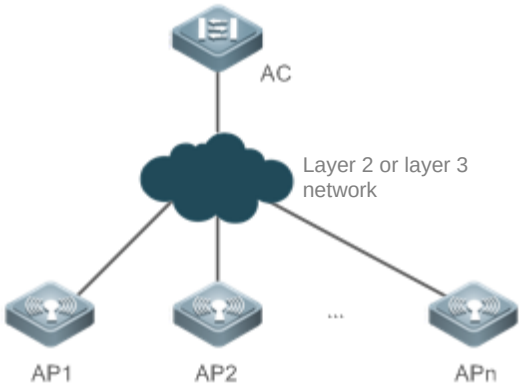
Command	**farpoint-steering enable**
Parameter Description	**enable**: Indicates that remote association information collection is enabled.
Defaults	By default, the remote association information collection function is disabled.
Command Mode	Enable remote association information collection for all AP groups in ap-config all mode and for a single AP group in ap-group mode.
Usage Guide	N/A

Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

Configuring Remote Association Information Collection

Scenario Figure 2-18	
Configuration Steps	● Enable remote association information collection on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)#ap-config all` `Ruijie(config-ap)# farpoint-steering enable` `Ruijie(config-ap)# ap-group test1` `Ruijie(config-group)#no farpoint-steering enable`
Verification	● Run **show running** to query the configuration information about remote association information collection.
	`Ruijie#show running-config` `ap-group test1` `!` `ap-group test2` ` farpoint-steering enable`

	! ap-group test3 farpoint-steering enable !

2.4.16 Configuring Automatic Device Information Upload

Configuration Effect

- Enable automatic upload of AC and AP software and hardware version information to the WIS cloud.

Notes

- If the WIS function is not enabled, AC and AP software and hardware version information will also be automatically uploaded after this function is enabled. The information upload priority is as follows:
- If the WIS client address is configured, the information is uploaded to the WIS client.
- If the WIS client is not configured but the device can access to the WIS public cloud, the information will be uploaded to the WIS public cloud.
- If the WIS client is not configured and the device cannot access to the WIS public cloud, the device information is not uploaded.

Configuration Steps

- Perform this operation in global configuration mode.

Command	**wis devinfo enable**
Parameter Description	**enable**: Indicates that device information is automatically uploaded.
Defaults	By default, automatic device information upload is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

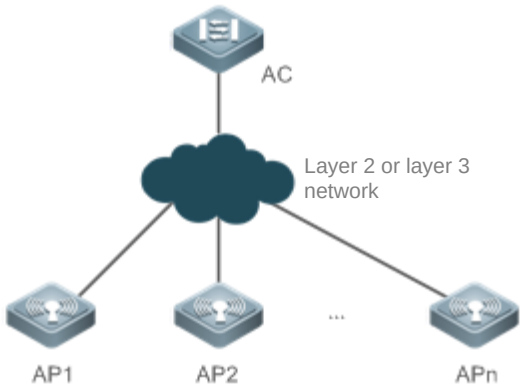
Verification

- Run **show running** to query the corresponding configuration.

Configuration Example

- N/A

Configuring Automatic Device Information Upload

Scenario **Figure 2-19**	
Configuration Steps	● Disable automatic device information upload on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)# no wis devinfo enable`
Verification	● Run **show running** to query the configuration information about automatic device information upload.
	`Ruijie#show running-config` `no wis devinfo enable!` `!`

2.5 Monitoring

Displaying

Function	Command
Display all configuration information.	**show running**
Display the configuration information of a specified AP.	**show ap-config running** *ap-name*
Display the radio information of all APs.	**show ap-config radio**
Display the configuration information of a specified AP's specified radio.	**show ap-config radio** *radio-id* **config** *ap-name*
Display the detailed status information of an AP's specified radio.	**show ap-config radio** *radio-id* **status** *ap-name*
Display the radio list of an AP.	**show ap-config radio status** *ap-name*
Display the running statistics of band selection.	**show band-select statistics**

Display the network optimization information.	**show wopt**

3 Configuring RF Scheduling

3.1 Overview

The radio frequency (RF) resources mentioned in this document include the RF of an Access Point (AP) as well as a wireless local area network (WLAN) services.

RF scheduling can perform automatic management on the RF resources.

RF scheduling can be used to disable the RF of an AP or a WLAN in the specified time interval, realizing the following functions:

- Reducing network traffic, saving network resources, and preventing waste or abuse of network resources
- Reducing RF interference and saving energy
- Disabling access services in a certain period to reduce potential security risks

RF scheduling can be used in the scenarios where wireless access services are required in specific time cycles.

3.2 Applications

Application	Description
AP RF Scheduling	In a fit AP architecture, enables and disables AP RF as scheduled.
WLAN Scheduling	In a fit AP architecture, enables and disables a WLAN as scheduled.

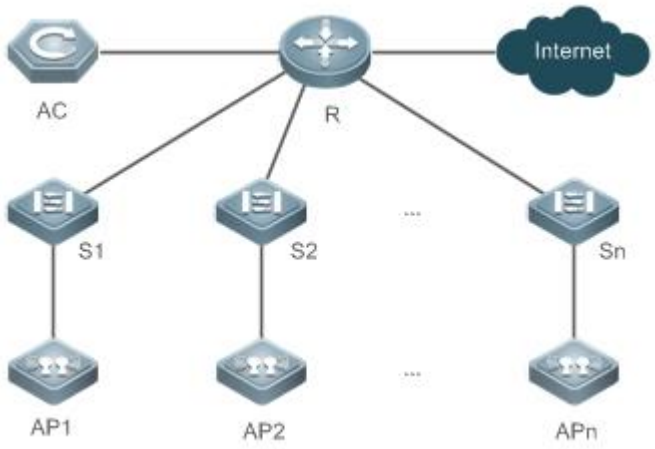
3.2.1 AP RF Scheduling

Scenario

In the scenario where access services need to be provided to wireless stations (STAs) in a specific time period, AP RF scheduling can be used to disable AP RF in the time period when no wireless STAs access the WLAN, thereby preserving network resources and saving energy.

The following figure shows the deployment of a WLAN in a teaching building of a university. The network architecture is a fit AP architecture. AP 1, AP 2, ……, and AP n are the access points located in different places of the building. In the daytime, wireless services need to be provided to students and teachers, but in the nighttime, such services are disabled. By using AP RF scheduling, AP RF of the entire building will be disabled automatically in the nighttime, and enabled again in the daytime. In this way, wireless services are available as scheduled while saving network resources and energy.

Figure 3-1



Deployment

In a fit AP architecture, you can configure AP RF on an AC.

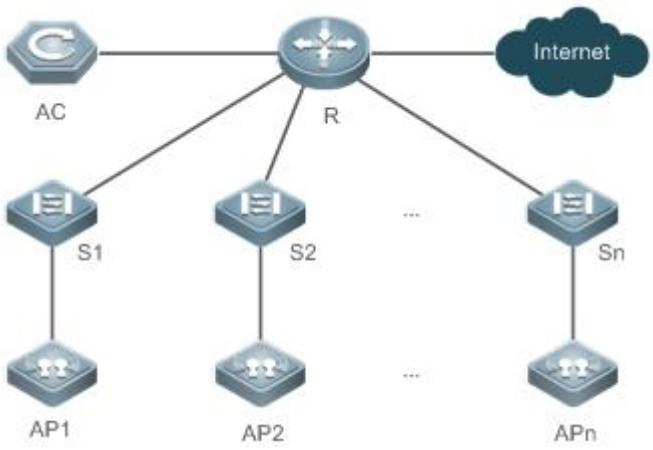
3.2.2 WLAN Scheduling

Scenario

Some WLANs of special use should be enabled only when needed to reduce interference of wireless RF and ensure security.

The following figure shows the deployment of the WLAN a bank business hall. The network architecture is a fit AP architecture. AP 1, AP 2, ……, and AP n are located in different places of the hall to provide free wireless access to customers. Typically, such kind of WLAN does not require a password and is available only during business hours. When WLAN scheduling is applied, the WLAN is automatically enabled during business hours, and disabled after work. In this way, the free customer-use WLAN is disabled, while other WLANs can continue to serve the bank clerks who are still working in the office.

Figure 3-2



Deployment

In a fit AP architecture, configure WLAN scheduling on an AC.

3.3 Features

Basic Concepts

Scheduling Session

A scheduling session indicates a time interval for an RF resource. A simple scheduling session contains only one time interval in a certain day; a complex scheduling session contains many duplicate time intervals in different dates. Currently, one scheduling session supports eight different (or same) time intervals.

For example, you can specify scheduling sessions as follows: 12:00–14:00 and 18:00–8:00 from Monday to Friday; 8:00–12:00 and 17:00–8:00 from Saturday to Sunday.

Overview

Feature	Description
Configuring a Scheduling Session	Specifies a scheduling session.
Scheduling AP RF	Applies a scheduling session to AP RF to enable or disable AP RF periodically.
Scheduling WLAN	Applies a scheduling session to a WLAN to enable or disable the WLAN periodically.

3.3.1 Configuring a Scheduling Session

Specify a scheduling session.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for RF scheduling. Then the scheduling session can be applied to an AP RF interface or WLAN.

Configuring a Scheduling Session

First, you need to create a scheduling session and specify the time and cycle.

For example, in the preceding example, if you want to provide wireless access services only in the daytime to teaching building, you can first create a scheduling session to specify the cycle as every day, and the scheduling interval as a period at night, for example, 21:00 to 6:00. If you want to provide WLAN services to customers of a bank only in the business hours of workdays, you can create a scheduling session to specify the cycle as workdays, and the scheduling time interval as off hours, for example, 18:00 to 9:00; and you can create the other cycle as weekends, and the scheduling interval as all day.

3.3.2 Scheduling AP RF

Enable or disable AP RF periodically.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for RF scheduling. Then you can apply the scheduling session to an AP RF interface.

When the scheduling session starts or ends, the system sends a scheduling message. The processing logic of the scheduling message will enable or disable the RF interface of an AP or the RF interfaces of an AP group where this scheduling session is applied.

Applying a Scheduling Session on an RF Interface

After a scheduling session is created, it must be applied to the corresponding AP RF interface so that the scheduling can take effect.

You can specify an AP RF interface in the following three ways:

- Based on all APs
- Based on an AP group
- Based on a single AP

In the preceding three approaches, you can specify a Radio ID for scheduling. If a Radio ID is not specified, the scheduling will be applied to all radios of the AP.

In the example of the teaching building, the AP RF needs to be specified based on actual conditions.

If all APs in this scenario are in the same group, or distributed in a few groups, the AP group-based configuration is recommended. If all the APs are located in the teaching building, the configuration based on all APs is also recommended. As the last choice, you can still specify the AP RF interface based on a single AP.

Handling of a Scheduling Message

After a scheduling session is created and the cycle and interval are specified, the system will start the timer of the scheduling session, and send a message after entering or exiting from this scheduling session. A scheduling message includes the following information:

- Scheduling Session ID
- Message type: the scheduling state, including entering and exiting from the scheduling session

The handling of a scheduling message covers all APs. The system will determine whether to start scheduling based on the priority of the scheduling Session ID configured for a single AP, AP group, and all APs.

Scheduling priority: The priority of a Session ID is as follows: AP-based Session ID > AP group-based Session ID > all APs-based Session ID. Namely, when a Session ID is configured for an AP, then the AP group-based Session ID and all APs-based Session ID will not take effect on this AP; if no Session ID is configured for an AP, the AP group-based Session ID will take effect; if no AP group-based Session ID is configured for an AP, the all APs-based Session ID will take effect.

If the effective scheduling Session ID of this AP RF is the same as that in the message, the message type will be checked. If in the scheduling state, the radio of this AP will be disabled. Otherwise, the radio will be enabled.

3.3.3 Scheduling WLAN

Enable or disable a WLAN periodically.

Working Principle

Before using the scheduling function, a scheduling session needs to be created first to specify the time for WLAN scheduling. Then the scheduling session can be applied to a WLAN.

When the scheduling session starts or ends, the system sends a scheduling message. In the handling of the scheduling message, the processing logic will locate the WLAN where this scheduling session is applied to, and enable or disable the WLAN.

Applying a Scheduling Session on an RF Interface

After the scheduling session is created, it must be applied to the corresponding WLAN so that the scheduling can take effect.

You need to specify in WLAN configuration mode the scheduling Session ID for the WLAN.

Handling of a Scheduling Message

After a scheduling session is created and the cycle and interval are specified, the system will start the timer of the scheduling session, and send a message after entering or exiting from this scheduling session. A scheduling message includes the following information:

- Scheduling Session ID
- Message type: entering or exiting from the scheduling session

The handling of a scheduling message covers all WLANs. The system will first check the session to which the WLAN is applied. If the scheduling Session ID to which the WLAN is applied is the same as that in the message, the message type will be checked. If in the scheduling state, the WLAN will be disabled. Otherwise, the radio will be enabled.

3.4 Configuration

Configuration	Description and Command	
Configuring AP RF Scheduling	⚠ (Mandatory) It is used to create a scheduling session, specify the time interval, and apply the scheduling session to an AP or AP group.	
	schedule session	Creates a scheduling session.
	schedule session time-range	Specifies the time interval of a scheduling session.
	schedule session	Applies the scheduling session to an AP or an AP group.
Configuring WLAN Scheduling	⚠ (Mandatory) It is used to create a scheduling session and apply it to a WLAN.	
	schedule session	Creates a scheduling session.
	schedule session time-range	Specifies the time interval of a scheduling session.
	schedule session	Applies the scheduling session to a WLAN.

3.4.1 Configuring AP RF Scheduling

Configuration Effect

- Create a scheduling session, specify a scheduling interval, and applies this scheduling session to an AP or an AP group to realize AP RF scheduling.

Configuration Steps

Creating a Scheduling Session

- (Mandatory) In global configuration mode, run the **schedule session** *sid* command to create a scheduling session. *sid* indicates Session ID, which can be set to a value ranging from1 to 64 on an AC, and from 1 to 8 on a fat AP.
- A scheduling session must first be created before use.
- The command must be run on the AC to enable scheduling.

Command	**schedule session** *sid*
Parameter Description	*sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP.
Defaults	By default, no scheduling session is created.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Time Interval for a Scheduling Session

(Mandatory) Run **schedule session** *sid* **time-range** *n* **period** { **everyday** | *day1* [**to** *day2*] } **time** { **all-day** | *hh1:mm1* **to** *hh2:mm2 }* to specify the time interval and cycle of a scheduling session.

- The function must be applied on the AC to enable scheduling.
- **session** *sid:* Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP.
- **time-range** *n*: Indicates the number of a time interval, which ranges from 1 to 8.
- **period** *day1* [**to** *day2*]: Indicates the scheduling cycle, where day1 indicates the start date, and day2 indicates the end date, which can be set to { sun | mon | tue | wed | thu | fri | sat }.

  to *day2*: By default, this parameter indicates that the scheduling cycle is one day.
- **period everyday**: Indicates that the session occurs every day, which is the simplified form of **period** *sun* **to** *sat*.
- **time** *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time period, and *hh1:mm1* and *hh2:mm2* indicate the start time and end time respectively in the unit of hours (ranging from 0 to 23) and minutes (ranging from 0 to 59).
- **time all-day**: Indicates that the session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.

Command	**schedule session** *sid* **time-range** *n* **period** { **everyday**	*day1* [**to** *day2*] } **time** { **all-day**	*hh1:mm1* **to** *hh2:mm2* }
Parameter Description	*sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP. *n*: Indicates the number of a time interval, which ranges from 1 to 8. *day1*: Indicates the start date of the scheduling session cycle, which can be set to { sun	mon	tue	wed	thu	fri	sat }. **to** *day2*: *day2* indicates the end date of the scheduling session cycle. By default, this parameter indicates that the scheduling cycle is one day. **everyday**: Indicates that the session occurs every day, which is the simplified form of **period** *sun* **to** *sat*.

	time *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time period, and *hh1:mm1* and *hh2:mm2* indicate the start time and end time respectively in the unit of hours (ranging from 0 to 23) and minutes (ranging from 0 to 59). **time all-day**: Indicates that the session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.
Defaults	No time period or cycle is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- The function must be applied on the AC to enable scheduling.
- In AP configuration mode, run the **schedule session** *sid* command to specify the Session ID for APs or a single AP. In AP group configuration mode, run the **schedule session** *sid* command to specify the Session ID for a AP group.
- After a scheduling session is applied, if the message for the scheduling session is displayed, the specified AP RF interface will automatically enter or exit from the scheduling state as specified by the massage type.

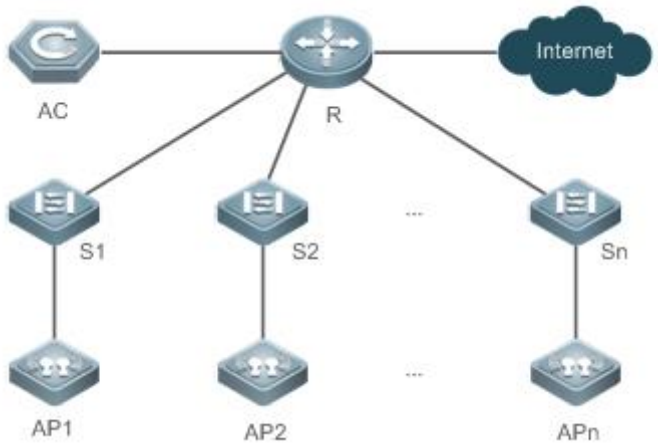
Command	**schedule session** *sid* [**radio** *radio-id*]
Parameter Description	*sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC. *radio-id*: Indicates ID of the radio on which the session is to be applied or deleted. The value ranges from 1 to the number of radios on the AP. By default, the value is set to the number of radios on the AP.
Defaults	No scheduling session is applied on a single AP, an AP group, or all APs.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** to display configurations on RF scheduling.
- Check whether scheduling is still performed for AP RF after a scheduling session expires.

Configuration Example

Providing WLAN Services to a Teaching Building of a University Only in the Daytime

Scenario **Figure 3-3**	 As shown in the figure, the fit AP architecture is used in this scenario, and only one AC is applied. All the APs in the teaching buildings belong to the same AP group, whose group ID is "class-room".
Configuration Steps	● Create a scheduling session on the AC. ● Specify the scheduling interval as in the nighttime. ● On the AC, apply the scheduling session to AP group "class-room".
AC	`AC# configure terminal` `AC(config)# schedule session 1` `AC(config)# schedule session 1 time-range 1 period sun to sat time 21:00 to 6:00` `AC(config)# ap-group class-room` `AC(config-ap-group)# schedule session 1`
Verification	● On the AC, run the **show running-config** command to display the configuration. ● Display the state of AP RF in the scheduling interval. ● Display the state of AP RF outside the scheduling interval.
AC	`AC# show running-config` `.....` `schedule session 1` `schedule session 1 time-range 1 period Sun to Sat time 21:00 to 06:00` `.....` `ap-group class-room` `.....` `schedule session 1` `.....`

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is not properly configured.
- The scheduling priorities on the AP are in conflict.
- Scheduling is not applied to the target radio.

3.4.2 Configuring WLAN Scheduling

Configuration Effect

- Create a scheduling session, specify a scheduling interval, and apply this scheduling session to a WLAN to realize WLAN scheduling.

Configuration Steps

Creating a Scheduling Session

- (Mandatory) In WLAN configuration mode, run the **schedule session** *sid* command to specify the scheduling Session ID of a WLAN.
- The command must be run on the AC to enable scheduling.
- After a scheduling session is applied, if the message for the scheduling session is displayed, the specified WLAN interface will automatically enter or exit from the scheduling state as specified by the massage type.

Command	**schedule session** *sid*
Parameter Description	**session** *sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP.
Defaults	No scheduling session is applied on a WLAN.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Time Interval for a Scheduling Session

- Mandatory.
- The function must be applied on the AC to enable scheduling.

Command	**schedule session** *sid* **time-range** *n* **period** { **everyday |** *day1* [**to** *day2*] } **time { all-day |** *hh1:mm1* **to** *hh2:mm2* }
Parameter Description	**session** *sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP. **time-range** *n*: Indicates the number of a time interval, which ranges from 1 to 8. **period** *day1*: Indicates the start date of the scheduling session cycle, which can be set to { sun | mon | tue | wed | thu | fri | sat }. **to** *day2*: *day2* indicates the end date of the scheduling session cycle. By default, this parameter indicates that the scheduling cycle is one day. **everyday**: Indicates that the session occurs every day, which is the simplified form of **period** *sun* **to** *sat*. **time** *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time period, and *hh1:mm1* and *hh2:mm2* indicate the start time and end time respectively in the unit of hours (ranging from 0 to 23) and minutes (ranging

	from 0 to 59). **time all-day**: Indicates that the session time range is a whole day, which is the simplified form of **time** *00:00* **to** *23:59*.
Defaults	By default, a scheduling session is not configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- The function must be applied on the AC to enable scheduling.

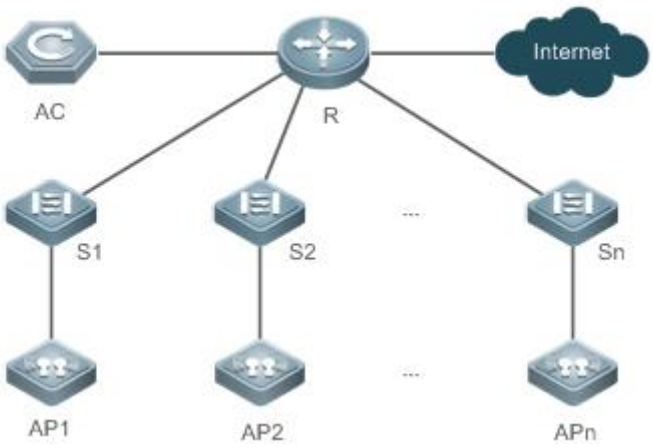
Command	**schedule session** *sid*
Parameter Description	**session** *sid*: Indicates Session ID. It can be set to a value ranging from 1 to 64 on an AC, and from 1 to 8 on a fat AP.
Defaults	By default, no scheduling session is configured. No scheduling session is applied on a WLAN or radio.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** to display configurations on RF scheduling.
- Check whether scheduling is still performed for a WLAN after a scheduling session expires.

Configuration Example

Providing WLAN Services to Customers in a Bank Only in the Daytime of Workdays

Scenario **Figure 3-4**	 As shown in the figure, the fit AP architecture is used in this scenario, and only one AC is applied. WLAN 99 is the customer-use WLAN, and the scheduling Session ID is "wlan bank-free". The APs include AP 1, AP 2, ……, and AP n.

Configuration Steps	● Create a scheduling session on the AC. ● On the AC, specify the scheduling intervals as the nighttime of workdays, and the whole weekends. ● On the AC, apply the scheduling session to WLAN 99.
AC	AC# configure terminal AC(config)# schedule session 1 AC(config)# schedule session 1 time-range 1 period mon to fri time 18:00 to 9:00 AC(config)# schedule session 1 time-range 2 period sat to sun time 00:00 to 23:59 AC(config)# wlan-config 99 AC(config-wlan)# schedule session 1
Verification	● On the AC, run the **show running-config** command to display the configuration. ● Display the state of the WLAN in the scheduling interval. ● Display the state of the WLAN outside the scheduling interval.
AC	AC# show running-config …… schedule session 1 schedule session 1 time-range 1 period mon to fri time 18:00 to 9:00 schedule session 1 time-range 2 period sat to sun time 00:00 to 23:59 …… wlan-config 99 wlan-bank-free …… schedule session 1 ……

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is not properly configured.

4 Configuring Band Select

4.1 Overview

Band Select is a technology for optimizing access band distribution for STAs on a WLAN.

The Band Select function leads dual-band STAs to access the higher-capacity 5 GHz band to reduce the pressure on the 2.4 GHz band and improve user experience.

The Band Select function is suitable for the following scenario: dual-band APs are used to provide coverage, and the two RF interfaces of the APs operate at 2.4 GHz and 5 GHz respectively; meanwhile, a WLAN is mapped to the two RF interfaces of the APs and provides access service at the two bands simultaneously.

Protocols and Standards

- IEEE 802.11

4.2 Applications

Application	Description
Band Select for a WLAN Using a Fit AP Architecture	In a fit AP architecture, a WLAN composed of multiple dual-band APs is enabled with the Band Select function.

4.2.1 Band Select for a WLAN Using a Fit AP Architecture

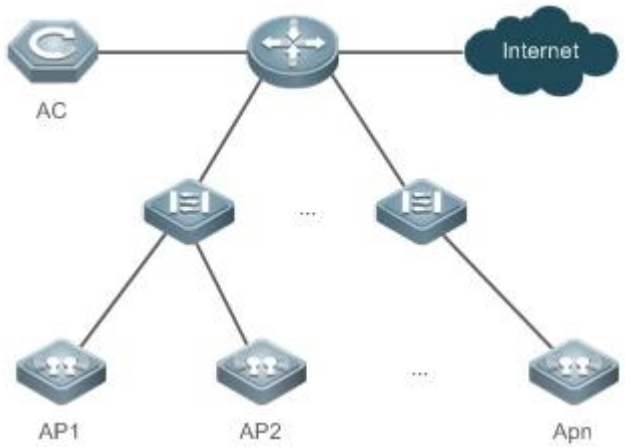
Scenario

In a fit AP architecture, a WLAN composed of multiple dual-band APs is enabled with the Band Select function,

as shown in Figure 4-1,

- One AC is associated with multiple dual-band APs. The AC and APs are connected through layer-2 switch devices and layer-3 routers.
- The WLAN is mapped to the two RF interfaces of all dual-band APs.

Figure 4-1



Remarks	AC is a wireless access controller. AP_1, AP_2 … AP_n are dual-band APs.

Deployment

- Manage parameters of the Band Select function on the AC.
- Apply the Band Select function, identifies STA types and leads STA access on the AC.

4.3 Features

Basic Concepts

IEEE802.11 Communication Band

IEEE802.11 comprises two communication bands:

- 2.4 GHz (2.4 to 2.4835 GHz), where 802.11b/g/n resides
- 5 GHz (5.15 to 5.35 and 5.725 to 5.825 GHz), where 802.11a/n resides

With the popularization of WLANs, there are more and more wireless users. Many users use dual-band wireless clients (STAs) supporting both 2.4 GHz and 5 GHz. However, 802.11b/g is more widely applied than 802.11a. Many dual-band STAs use 2.4 GHz, causing congestion of 2.4 GHz and waste of 5 GHz. Actually, the 5 GHz band has a greater access capacity. The 2.4 GHz band has up to three non-overlapped channels, whereas the 5 GHz band provides more non-overlapped channels.

STA Scanning

There are two modes, namely, passive scanning and active scanning.

- Passive scanning: An STA monitors beacon frames sent by nearby APs on all channels of all supported bands. The beacon frames contain WLAN access information. The STA parses the information to learn about the WLANs that are available nearby.
- Active scanning: The STA broadcasts a Probe Request frame on all channels of all supported bands. After receiving the Probe Request frame, the APs providing WLAN access service sends a Probe Response frame including some WLAN information to the STA.

Generally, the STA summarizes the SSIDs of all discovered WLANs and provides an accessible WLAN list for users.

Dual-band STA

WLAN network interface cards (WNICs) used by STAs to connect to WLANs are classified into a, b, g and n types, which indicate the 802.11 protocol types supported by the WNICs. 802.11a operates at 5 GHz, 802.11b/g at 2.4 GHz, and 802.11n at 5 GHz and 2.4 GHz.

Therefore, if the specification of a WNIC includes both a and b/g, this WNIC supports both the two bands, namely, a dual-band STA. A dual-band STA can access both the 5 GHz band and the 2.4 GHz band.

Dual-band AP

A dual-band AP is able to access two bands. Therefore, a dual-band AP requires at least two RF interfaces, one for 5 GHz and the other for 2.4 GHz.

A WLAN enabled with Band Select must be mapped to the two RF interfaces of the dual-band AP and provides access service at the two bands.

Overview

Feature	Description
Identifying STA Types	The Band Select function identifies whether an STA is a dual-band STA.
Controlling the Active Scanning Process	The Band Select function controls active scanning of the dual-band STA to prevent the STA from discovering WLANs of the 2.4 GHz band.
Rejecting Accessing the 2.4 GHz Band	The Band Select function rejects the dual-band STA from accessing the 2.4 GHz band and improves the chance of accessing the 5 GHz band.

4.3.1 Identifying STA Types

To lead a dual-band STA to access the 5 GHz band, you should first identify whether the STA is a dual-band STA; that is, identify the band supported by the STA.

Working Principle

Active scanning is an approach for an STA to discover WLANs. When using active scanning, the STA sends a Probe Request frame on each supported channel. If the channel information in the Probe Request frame sent by the STA can be obtained, the bands supported by the STA can be identified.

For example, if an AP receives the Probe Request frame on channels 1-13, the AP learns that the STA supports the 2.4 GHz band. If the AP receives the Probe Request frame on channels 149-165, the AP learns that the STA supports the 5 GHz band.

Since a single-band AP can receive the Probe Request frame only at one band, only a dual-band AP can correctly identify the STA type. This is why the Band Select function requires a dual-band AP be used.

STA Classification Standards

A dual-band AP classifies STAs based on the following standards:

- If the AP can receive the Probe Request frame from an STA both at the 2.4 GHz band and the 5 GHz band, this STA is a dual-band STA.

- If the AP can receive the Probe Request frame from this STA only at the 5 GHz band, the AP learns that this STA is a 5 GHz STA.
- If the AP can receive the Probe Request frame from this STA only at the 2.4 GHz band, the AP learns that this AP is a 2.4 GHz STA.

The AP must wait for a period of time to verify that no Probe Request frame is received at the band; therefore, identifying a single-band STA is time-consuming but does not affect the normal use by users. Among the three types of STAs, the first two types are called the dual-band STAs in the Band Select function and the last type is called the inhibition STAs.

It takes a period of waiting time (fixed to 2 seconds) to determine whether a Probe Request frame is sent at the 5 GHz band. Due to different STA drivers, this time is not applicable to all dual-band STAs. Therefore, STA types may not be correctly identified in the beginning. As long as dual-band STAs can send Probe Request frames at the 5 GHz band later, the correct STA types can be identified.

STA Information Saving

The STA information identified by a dual-band AP must be saved to provide the basis for subsequent responding policies.

Since Probe Request frames sent by STAs are broadcast packets, an AP may receive many Probe Request frames generally. It is unnecessary to save all the frames because some distant STAs may not access the AP. Therefore, the Band Select function saves only the information of STAs that may have access. The selection criterion is the Received Signal Strength Indication (RSSI) of STAs. Only those whose RSSI exceeds a threshold can access the AP, and only then does the identified information need to be saved.

STA Information Aging

Users can configure the bands supported by some STAs; therefore, STA type may change during use.

Take an 802.11a/g/n-supported WNIC for example. The WNIC works as a dual-band STA in the beginning. However, a user disables its 802.11a mode or the support for the 5 GHz channels. Then, the WNIC changes to a single-band 2.4 GHz STA.

In this case, an aging mechanism needs to be used for the identified STA information. After a period of time, the previously identified STA information is discarded.

4.3.2 Controlling the Active Scanning Process

After identifying the bands supported by an STA, a dual-band AP can control the active scanning of the STA according to the STA information. The purpose is to prevent a dual-band STA from discovering 2.4 GHz WLANs and thus lead the dual-band STA to access the 5 GHz band.

Working Principle

During active scanning, the STA broadcasts a Probe Request frame. After receiving the Probe Request frame, an AP sends a Probe Response frame immediately to inform the STA of the accessible WLANs on this AP. During active scanning of a dual-band STA, the STA sends a Probe Request frame and waits for a Probe Response frame on the two bands. After the Band Select function is enabled, the AP controls the active scanning and adopts different response approaches according to actual situations.

Active Scanning Before the Band Select Function Identifies STA Types

If the Band Select function is enabled for a WLAN, the WLAN may have different responses to active scanning of an STA. Before STA types are identified:

- The AP does not respond to Probe Request frames from the 2.4 GHz band.
- The AP responds to Probe Request frames from the 5 GHz band.

After receiving a Probe Request frame from the 2.4 GHz band, the AP cannot determine whether the STA supports the 5 GHz band. To prevent the STA from discovering that the WLAN provides access service at the 2.4 GHz band, the AP responds after the identification process ends.

If the AP receives a Probe Request frame from the 5 GHz band, it indicates that the STA supports the 5 GHz band. In this case, the AP sends a Probe Response frame immediately to tell the STA that WLAN provides access service at the 5 GHz band.

↘ Active Scanning After the Band Select Function Identifies STA Types

When the AP receives a Probe Request frame after identifying the STA type, the AP can find the source MAC address in the Probe Request frame stored on the AP.

- If the STA is a dual-band STA, the AP does not respond to a 2.4 GHz Probe Request; if the STA is an inhibition STA, the AP responds negatively
- The AP responds to a 5 GHz Probe Request .

Not responding to a 2.4 GHz Probe Request sent by a dual-band STA can prevent the dual-band STA from discovering that a WLAN provides access service at the 2.4 GHz band. In this way, the dual-band STA only discovers that the WLAN provides access service at the 5 GHz band. The dual-band STA has to select the 5 GHz band for access.

The AP must responds to the 2.4 GHz Probe Request from an inhibition STA. Since an inhibition STA supports only the 2.4 GHz band, the inhibition STA cannot identify a WLAN if the AP does not respond to the 2.4 GHz Probe Request. However, the response to an inhibition STA is negative.

A 5 GHz Probe Request is sent only by a dual-band STA. Therefore, the AP must send a Probe Response immediately to tell the WLAN to provide access service at the 5 GHz band.

↘ Negative Response to an Inhibition STA

The Band Select function always positively responds to 5 GHz Probe Requests, does not respond to 2.4 GHz Probe Requests sent by dual-band STAs, and responds to Probe Requests from inhibition STAs negatively.

Figuratively speaking, a negative response is a discounted response. For example, when receiving multiple Probe Requests consecutively, the AP sends only one Probe Response.

The negativity depends on two parameters: STA scanning cycle threshold and the probe count of the inhibition STA.

The STA scanning cycle refers to the time for scanning all supported channels during the active scanning of an STA. This time depends on the driver of the STA and varies with STAs. The STA scanning cycle is a value configured by users, which is considered the minimum STA scanning cycle. If the scanning cycle of an STA is smaller than this value, two consecutive scanning cycles may be considered to be one by an AP. This parameter is useful when some STAs send multiple Probe Requests within one scanning cycle.

Example: Assume that an STA scans all channels every 150 milliseconds and sends two Probe Request frames consecutively on each channel. If an AP does not specify the minimum scanning cycle of the STA, the AP cannot identify whether the STA sends two frames within the same scanning cycle or sends the two frames in two consecutive scanning cycles. If the AP sets the minimum scanning cycle of the STA to 200 milliseconds, the two frames are considered to be

sent within the same scanning cycle because their interval is shorter than 200 milliseconds. The probe count of the STA on the AP is 1. Since the specified minimum scanning cycle (200 milliseconds) and the actual scanning cycle (150 milliseconds) are different, the counts are also different. Assume that the STA performs scanning for three consecutive cycles, the count on the AP will be 2 because the first two cycles are considered to be one. However, this problem does not cause inconvenience to users.

The probe count of an STA reflects the negativity of the response. This parameter indicates that an AP sends one response after an inhibition STA performs active scanning for multiple cycles. For example, if the default value is 2, the WLAN on the AP sends a Probe Response frame after the STA performs scanning for two consecutive cycles.

4.3.3 Rejecting Accessing the 2.4 GHz Band

⚠ The Band Select function controls only the active scanning of an STA, but cannot prevent the STA from discovering a 2.4 GHz WLAN through passive scanning. Therefore, some dual-band STAs can still discover 2.4 GHz WLANs and attempt to access the WLANs. In this case, the Band Select function may fail.

The Band Select function can reject 2.4 GHz access requests from dual-band STAs to improve the chance for dual-band STAs accessing the 5 GHz band.

⚠ Rejecting a dual-band STA's 2.4 GHz access request helps facilitate the Band Select function; however, the Band Select function cannot be 100% successful.

Working Principle

After an STA discovers a WLAN for a user to access the WLAN, the STA sends an Authentication Request to the AP at first. Then, the AP sends an Authentication Response to permit or reject the STA's authentication request.

The Band Select function processes the Authentication Request. If the Authentication Request is sent by a dual-band STA at the 2.4 GHz band, the function can reject the Authentication Request until the dual-band STA sends an Authentication Request from the 5 GHz band. Thus, the STA is led to access the 5 GHz band.

Generally, when a dual-band STA searches for access, the STA sends one or more Authentication Requests at a band and waits for responses. If the STA does not receive responses or fails in access, the STA sends Authentication Requests at the other band and waits for responses. However, some dual-band STAs send Authentication Requests only at the 2.4 GHz. For high availability, you can use the Band Select function to set the rejecting count for a dual-band STA.

Assume that a dual-band STA sends Authentication Requests for M times before changing the band, and the rejecting count is set to N. If the dual-band STA attempts to access the 5 GHz band at first, the STA can access the 5 GHz band immediately. If the dual-band STA attempts to access the 2.4 GHz band at first, the STA can access the 5 GHz band only if N is equal to or greater than M; otherwise, the STA accesses the 2.4 GHz band. No matter which band a dual-band STA accesses, if the dual-band STA attempts to access the 2.4 GHz band at first, min (smaller one between M and N) Authentication Requests are rejected or ignored. As a result, the STA's access is delayed. The delay time depends on the driver of the STA. For example, if the STA sends Authentication Requests at the interval of 100 milliseconds and four Authentication Requests are ignored, the access of the STA will be delayed for 400 milliseconds.

⚠ When the Band Select function rejects the access request of a dual-band STA while another access control module such as load balance accepts the access request, the STA will still gain access. This is because the Band Select function plays only the "leading" role during STA access and has a low priority. When the Band Select function conflicts with other functions, the other functions shall prevail.

4.4 Configuration

Configuration	Description and Command	
Configuring Band Select	(Mandatory) It is used to enable the Band Select function for a WLAN.	
	band-select enable	Enables the Band Select function.
	(Optional) It is used to set the parameters of the Band Select function.	
	band-select acceptable-rssi	Configures the minimum RSSI for the Band Select function.
	band-select access-denial	Configures the rejecting count for a dual-band STA's 2.4 GHz access requests.
	band-select age-out	Configures the aging time of STA information.
	band-select probe-count	Configures the probe count of an inhibition STA.
	band-select scan-cycle	Configures the scanning cycle threshold of an STA

4.4.1 Configuring Band Select

Configuration Effect

- Enable the Band Select function for a WLAN to lead dual-band STAs to access the 5 GHz band.

Notes

- N/A

Configuration Steps

Enabling the Band Select Function for a WLAN

- Mandatory.
- If there is no special requirement, enable this function on an AC or a fat AP.

Command	band-select enable
Parameter Description	N/A
Defaults	The Band Select function is disabled.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Configuring the Minimum RSSI for the Band Select Function

- (Optional) It is configured when you want to adjust the coverage of the Band Select function.

- If there is no special requirement, enable this function on an AC or a fat AP.
- The higher the value, the smaller the coverage of the Band Select function; the lower the value, the larger the coverage of the Band Select function. However, if the value exceeds a certain limit, the STA signals that gain access may be too weak, causing the connection rate of the entire network to slow down.

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Specifies the minimum SSID for the Band Select function, ranging from -100 to -50 dBm.
Defaults	The default value is -80 dBm
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rejecting Count for a Dual-Band STA's 2.4 GHz Access Requests

- (Optional) It is configured when it is necessary to reject the 2.4 GHz access request of dual-band STAs. If many STAs fail in access or it takes much time to access, configure this parameter to a smaller value or to 0.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The more the rejecting count is, the more difficult the dual-band STA accesses the 2.4 GHz band, and the later the STA accesses the 2.4 GHz band. On the other hand, the less the rejecting count is, the easier the dual-band STA accesses the 2.4 GHz band, and the sooner the STA accesses the 2.4 GHz band.

Command	**band-select access-denial** *value*
Parameter Description	*value*: Specifies the rejecting count for a dual-band STA's 2.4 GHz access requests, ranging from 0 to 10.
Defaults	The default value is 2
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Aging Time of STA Information

- (Optional) If no dual-band STAs change to single-band 2.4 GHz STAs, configure a longer aging time. Otherwise, configure a shorter aging time. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The longer the STA information aging time, the longer the lifecycle of STA information, and the less sensitive of an AP to STA's band change. The shorter the STA information aging time, the shorter the lifecycle of STA information, and the more sensitive of an AP to STA's band change.

Command	**band-select age-out** { **dual-band** *value* **| suppression** *value* }
Parameter Description	**dual-band** *value*: Specifies the aging time of dual-band STA information, ranging from 20 to 120 seconds. **suppression** *value*: Specifies the aging time of inhibition STA information, ranging from 10 to 60 seconds.
Defaults	The aging time of dual-band STA information is 60 seconds and the aging time of inhibition STA information is 20 seconds.

Command Mode	Global configuration mode
Usage Guide	It is recommended that the aging time of dual-band STA information be set to twice or three times that of inhibition STA information.

Configuring the Probe Count of an Inhibition STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The greater the probe count of an STA, the stronger inhibition the Band Select function performs on an inhibition STA, and the more difficult the inhibition STA discovers a WLAN. On the other hand, the smaller the probe count of an STA, the weaker inhibition the Band Select function performs on an inhibition STA, and the easier the inhibition STA discovers a WLAN.

Command	**band-select probe-count** *value*
Parameter Description	*value*: Specifies the probe count of an inhibition STA, ranging from 1 to 10.
Defaults	The default value is 2.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Scanning Cycle Threshold of an STA

- (Optional) If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value. If it is uncertain, use the Defaults.
- If there is no special requirement, enable this function on an AC or a fat AP.
- The greater the scanning cycle threshold of an STA, the more slowly the probe count of the STA increases, and the more difficult the STA discovers a WLAN. On the other hand, the smaller the scanning cycle threshold of the STA, the more quickly the probe count of the STA increases, and the easier the STA discovers a WLAN.

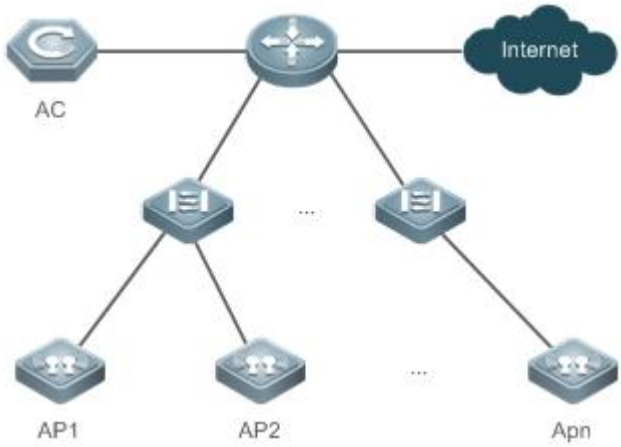
Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Specifies the scanning cycle threshold of an STA, ranging from 1 to 1000 milliseconds.
Defaults	The default value is 200 milliseconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command to display parameters of the Band Select function.
- Run the **show running-config** command to check whether the Band Select function is enabled.
- After a period of running, run the **show band-select statistics** command to check the statistics on the AC.
- Check whether the Band Select function controls the active scanning process by capturing packets.

Configuration Example

Configuring Band Select for a WLAN Using a Fit AP Architecture

Scenario **Figure 4-2**	 Figure 4-2 shows a typical WLAN using a fit AP architecture. ● AC is a wireless access controller. ● AP_1, AP_2 … AP_n are dual-band APs. ● The AC and APs are connected through layer-2 switch devices and layer-3 routers. ● The WLAN for which the Band Select function needs to be enabled is WLAN 99, whose SSID is wlan-band select. This WLAN is mapped to the two RF interfaces of all dual-band APs.
Configuration Steps	● (Optional) Configure the parameters of the Band Select function on the AC. ● Enable the Band Select Function for WLAN 99 on the AC.
AC	AC# configure terminal AC(config)# wlan-config 99 AC(config-wlan)# band-select enable
Verification	Access WLAN "wlan-band select" by using a dual-band STA. ● The STA accesses the 5 GHz band. (The STA may also access the 2.4 GHz band upon band selection failure.) ● Check the statistics of the Band Select function on the AC. The count should increase.
AC	A# show band-select statistics Band Select Statistics Number of dual band client..... 1 Number of dual band client added..... 1 Number of dual band client expired..... 0 Number of suppressed client..... 0 Number of suppressed client added..... 0 Number of suppressed client expired..... 0

Common Errors

- The parameters are improper.

- The Band Select function is not enabled.
- One of the two RF interfaces of a dual-band AP is disabled.

4.5 Monitoring

Displaying

Description	Command
Displays the configuration of the Band Select function.	**show band-select configuration**
Displays the statistics of the Band Select function.	**show band-select statistics**

5 Configuring CorrectLink

5.1 Overview

CorrectLink provides an intelligent WLAN clients access solution to identify and guide access behaviors of clients, so that clients can access APs with the optimal performance.

At present, correctLink can perform guidance of 5 GHz preferred, remote association, and load balancing on clients.

The purpose of 5 GHz preferred is to guide clients with 5 GHz capabilities to associate with the 5 GHz signals for better experience.

The purpose of remote association is to prevent clients from associating with overlow-RSSI signals.

The purpose of load balancing is to make clients access lower-load APs when guaranteeing that no remote association occurs.

5.2 Applications

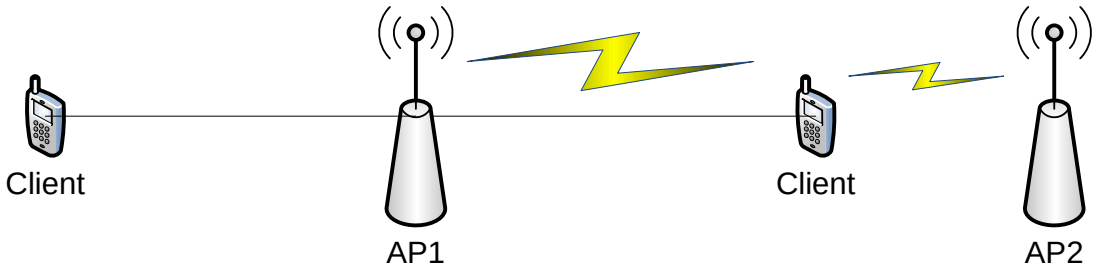
Application	Description
Remote Association	A client is not connected to a near AP, but a far AP. In this case, the client's uplink transmission works at a low rate with poor signals, resulting in poor wireless experience. Remote association can make the client associate with a stronger-signal AP.
5 GHz Preferred	A dual-band client does not select the 5 GHz frequency band, but the 2.4 GHz frequency band. The 2.4 GHz frequency band provides a small number of channels and limited channel resources. It guarantees good client experience in idle time, but degrades client experience in peak-load hours. 5 GHz preferred can guide clients supporting 5 GHz to the 5 GHz frequency band.
Load Balancing	The distribution density of clients is out of control, and client experience is restricted by the access density. In a network environment, even if the network optimization parameters are optimal and clients are connected to the nearest APs and the 5 GHz frequency band, a high access density may degrade the air interface service quality and ultimately affect client experience.

5.2.1 Remote Association

Scenario

As shown in the following figure, a client is not connected to a near AP, but a far AP. In this case, the client's uplink transmission works at a low rate with poor signals, resulting in poor wireless experience. Remote association can make the client associate with a stronger-signal AP.

Figure 5-1



Deployment

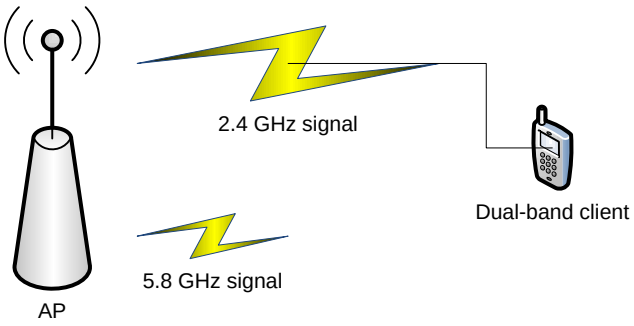
- Enable correctLink to resolve remote association issues.

5.2.2 5 GHz Preferred

Scenario

As shown in the following figure, a dual-band client does not select the 5 GHz frequency band, but the 2.4 GHz frequency band. The 2.4 GHz frequency band provides a small number of channels and limited channel resources. It guarantees good client experience in idle time, but degrades client experience in peak-load hours. 5 GHz preferred can guide clients supporting 5 GHz to the 5 GHz frequency band.

Figure 5-2



Deployment

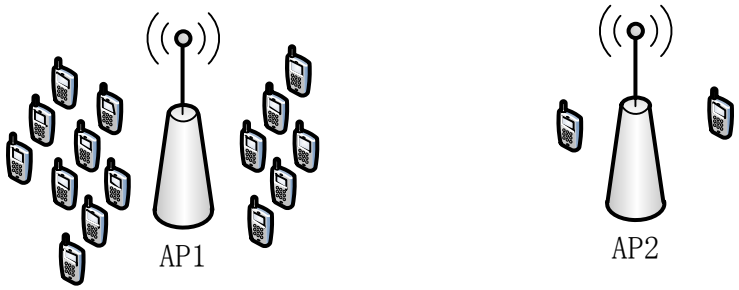
- Enable correctLink to resolve 5 GHz preferred issues.

5.2.3 Load Balancing

Scenario

As shown in the following figure, the distribution density of clients is out of control, and client experience is restricted by the access density. In a network environment, even if the network optimization parameters are optimal and clients are connected to the nearest APs and the 5 GHz frequency band, a high access density may degrade the air interface service quality and ultimately affect client experience.

Figure 5-3



Deployment

- Enable correctLink to resolve load balancing issues.

5.3 Features

Basic Concepts

correctLink

correctLink is a technology that guides clients to achieve the optimal access state, and provides guidance of remote association, 5 GHz preferred, and load balancing.

Overview

Feature	Description
correctLink	Guides clients to achieve the optimal access state.

5.3.1 correctLink

During client access, perform guidance of remote association, 5 GHz preferred, and load balancing on clients, so that the clients achieve the optimal access state.

Working Principle

Judge whether a client accesses the optimal AP based on the information detected during client association and correctLink rules. If the client fails to access the optimal AP, guide access of the client.

correctLink rules:

If the difference between the detected AP RSSI and the highest RSSI is less than 10 dBm (default value), the set of APs is called an APset. If the load of an AP included in the APset is less than that of the currently-accessed AP by a value more than 5 (default value), a Cset exists.

If the currently accessed AP does not belong to the APset, the current access is not optimal, and the client cannot access the AP.

If the currently accessed AP belongs to the APset but the Cset is not null, the current access is not optimal, and the client cannot access the AP.

If the currently accessed AP belongs to the APset and the Cset is null, the current access is optimal, and the client can access the AP.

5.4 Configuration

Configuration	Description and Command	
Configuring correctLink	(Optional) It is used to guide client access.	
	clink enable	Enables correctLink.
	clink rssi-delta-threshold	Configures the remote association RSSI difference threshold of correctLink.
	clink lb-client-threshold	Configures the load balancing judgment threshold of correctLink.
	clink lb-client-delta-threshold	Configures the load balancing difference threshold of correctLink.
	clink bandsel-5g-rssi-threshold	Configures the 5G preferred RSSI threshold of correctLink.
	clink bandsel-5g-client-threshold	Configures the 5 GHz preferred load threshold of correctLink.
	clink max-fails	Configures the rate-limiting attempt threshold of correctLink.

5.4.1 Configuring correctLink

Configuration Effect

- Enable correctLink to identify and guide client based on correctLink rules.

Notes

- If APs in an area belong to different ACs and do not join the virtual AC group, correctLink takes effect only between APs on the same AC, but not across ACs. That is, correctLink does not guarantee the global guiding effect, but only between APs on the same AC.
- If correctLink is configured only on some AP groups, it takes effect only between APs in these AP groups. correctLink does not guarantee the global guiding effect.

Enabling correctLink

- Enable correctLink in global configuration mode or AP group configuration mode.
- After the global configuration takes effect, correctLink applies to all AP groups. However, the **show running** command in the AP groups does not display the configurations.
- When correctLink is configured for a single AP group, the **show running** command in the AP group can display the configurations.
- When the global configuration is enabled, correctLink cannot be configured for a single AP group. To configure correctLink for a single AP group, disable the global configuration first.

Command	**clink enable**
Parameter Description	**enable**: Enables correctLink.

Defaults	correctLink is disabled by default.
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	N/A

Configuring the Remote Association RSSI Difference Threshold of correctLink

- After the remote association RSSI difference threshold is configured, when the difference between the uplink associated RSSI of the client and the detected highest RSSI is greater than the threshold, it is determined that the client is a remote client and cannot access the AP.

Command	**clink rssi-delta-threshold** *thrd*
Parameter Description	*thrd*: Indicates the RSSI difference threshold.
Defaults	10
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Load Balancing Judgment Threshold of correctLink

- With load balancing enabled, when the load of clients associated with the AP exceeds the load balancing judgment threshold, load balancing judgment is performed.

Command	**clink lb-client-threshold** *thrd*
Parameter Description	*thrd*: Indicates the load balancing judgment threshold.
Defaults	30
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Load Balancing Difference Threshold of correctLink

- When a client detects APs, if the difference between an AP's RSSI and the detected highest RSSI is less than the remote association RSSI threshold, the set of these APs is called an APset.
- After the load balancing difference threshold is configured, it is determined that load imbalance exists and a current client cannot access AP X when all of the following conditions are met:

1. The number of clients associated with AP X is greater than the load balancing enabling threshold.
2. An APset exists and AP Y unassociated with the current client exists in the APset.
3. The number of clients associated with AP Y is less than the number of clients associated with AP X by a value higher than the load balancing difference threshold.

Command	**clink lb-client-delta-threshold** *thrd*
Parameter Description	*thrd*: Indicates the load balancing difference threshold.
Defaults	5
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring the 5G Preferred RSSI Threshold of correctLink

- After the 5 GHz preferred RSSI threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and the RSSI of 5 GHz signals is greater than the threshold in the WLAN, the client cannot be associated with the WLAN in the 2.4 GHz frequency band.

Command	**clink bandsel-5g-rssi-threshold** *thrd*
Parameter Description	*thrd*: Indicates the 5 GHz preferred RSSI threshold.
Defaults	20
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the 5 GHz Preferred Load Threshold of correctLink

- After the 5 GHz preferred load threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and load of 5 GHz signals is less than the threshold in the WLAN, the client cannot be associated with the WLAN in the 2.4 GHz frequency band.

Command	**clink bandsel-5g-client-threshold** *thrd*
Parameter Description	*thrd*: Indicates the 5 GHz preferred load threshold.
Defaults	100
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rate-limiting Attempt Threshold of correctLink

- After a client is rate-limited for a certain number of times equal to the rate-limiting attempt threshold, stop rate limiting to guarantee access experience of the client.

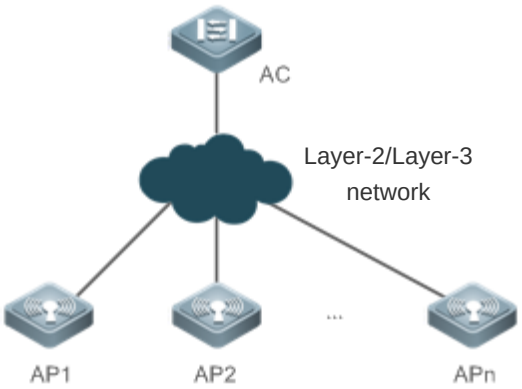
Command	**clink max-fails** *thrd*
Parameter Description	*thrd*: Indicates the rate-limiting attempt threshold.
Defaults	2
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the configurations.

Configuration Example

Enabling correctLink and Configuring the Remote Association RSSI Difference Threshold to 7

Scenario Figure 5-4	
Configuration Steps	● Enable correctLink globally on the AC. ● Configure the remote association RSSI difference threshold to 7 on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)#clink enable` `Ruijie(config)#clink rssi-delta-threshold 7`
Verification	Display the configurations after enabling correctLink for verification. ● Run the **show running** command to display the configurations.
	`Ruijie#show running-config` `!` `clink enable` `clink rssi-delta-threshold 7` `!`

5.5 Monitoring

Displaying

Description	Command
Displays all configuration information.	**show running**
Displays the correctLink result.	**show clink result**
Displays the correctLink statistics.	**show clink statistic**
Displays the probe information.	**show clink probe**

6 Configuring Smartant

6.1 Overview

Smartant means smart antenna, also known as auto-sensing antenna array. It is composed of three parts: antenna array, beam forming network, and beam forming algorithm. By adopting algorithms meeting certain criteria, Smartant adjusts the weighted amplitude and phase of each array signal and thereby adjusts the radiation pattern of the antenna array to enhance required signals and suppress interference signals.

Smartant can solve network interference and signal fading and increase system capacity.

Smartant is usually used in a complex environment where, for example, a lot of obstacles or certain interferences exist.

6.2 Applications

Application	Description
Obstacle environment	Certain obstacles exist in a wireless network environment.

6.2.1 Obstacle Environment

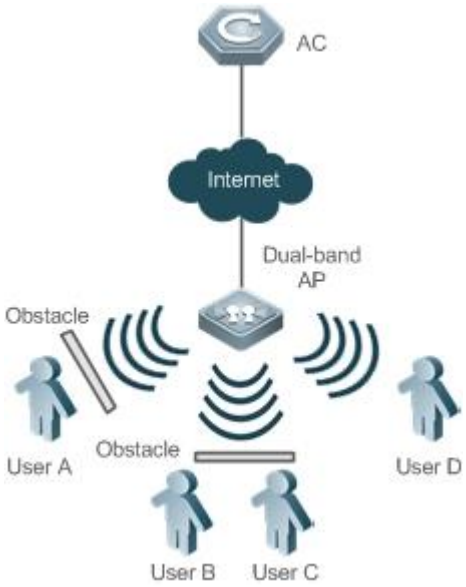
Scenario

Certain obstacles exist in a wireless network environment, for example, load bearing walls and glass windows.

The networking topology is shown as follows:

- Wireless stations (STAs) are evenly distributed around the AP.
- The Smartant function is enabled by default.
- Obstacles exist between certain STAs and the AP.

Figure 6-1 Networking Topology of Smartant



Deployment

- The AP performs downlink wireless packet training and collects data required by Smartant.
- Based on the collected data for Smartant, the AP executes the beam forming algorithm to compute an optimal antenna path for each STA.
- The AP sends data to each STA by the computed optimal path.

6.3 Features

Basic Concepts

Smartant

Based on beamwidth, antennas are divided into omni-directional and directional. Omni-directional antennas usually provide a wide horizontal coverage but a narrow distance, which is contrary to directional antennas. Smartant combines the advantages of both omni-directional and directional antennas. It can cover 360 degree horizontal radiation with a longer distance at each angle.

Wireless Packet Training

Smartant samples STA communication packets for training. When an STA transmits downlink traffic, Smartant changes the direction of packet transmission by setting the transmitting antennas, extracts the rates of packet loss in different antenna directions for evaluation, and finally computes an optimal path for antenna transmission based on the beam forming algorithm.

Overview

Feature	Description
Smartant path selection	Finds an optimal transmission path between the AP and STAs for the best performance.

6.3.1 Smartant Path Selection

With Smartant enabled, the AP can find an optimal transmission path for each STA.

Working Principle

Through downlink packet training and sampling by the AP, an optimal transmission path is found to avoid interferences and obstacles.

6.4 Configuration

Configuration	Description and Command	
Enabling the Smartant function	⚠ (Optional) It is used to configure the Smartant function.	
	smartant enable radio	Configures Smartant.

6.4.1 Configuring Smartant

Configuration Effect

- Configure the Smartant status.

Notes

- If the current device does not support Smartant, the configuration cannot take effect. Currently, Smartant is supported on the following models: AP320-I.

Configuration Steps

↘ Configuring Smartant for a Specified Radio of a Specified AP

- (Optional) Use the **smartant enable radio** *radio-id* command to configure Smartant for a specified in AP configuration mode.
- Except otherwise required, only Smartant-capable APs support Smartant.
- Smartant is configured on per-radio and per-AP basis.

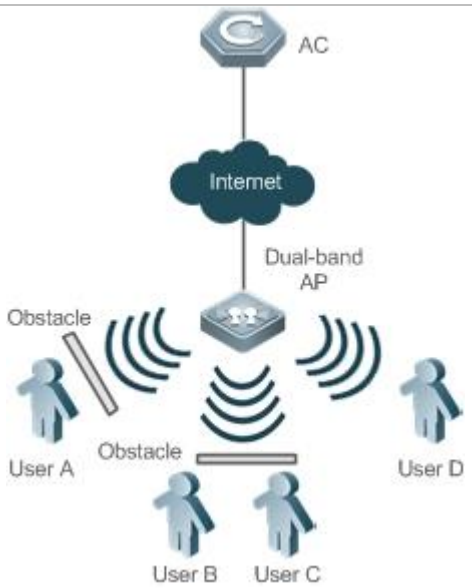
Command	**[no] smartant enable radio** *radio-id*
Parameter Description	*radio-id*: ID of the radio to be configured
Defaults	The Smartant function is enabled by default.
Command Mode	AP configuration mode
Usage Guide	This command is used to enable or disable the Smartant function. For Smartant-incapable devices, the configuration cannot take effect.

Verification

- Run the **show ap-config running** *ap-name* command to verify the configuration.

Configuration Example

↘ Configuring Smartant for a Specified Radio of a Specified AP

Scenario **Figure 6-2**	
Configuration Steps	● Configure Smartant for a specified Radio on a specified AP.
	`Ruijie# configure terminal` `Ruijie(config)#ap-config ap320` `Ruijie(config-ap)#smartant enable radio 1`
Verification	After the Smartant function is configured for the specified radio of the specified AP, check the configuration through the following ways. ● Run the **show ap-config running** *ap-name* command to check the configuration. Because Smartant is enabled by default, the **enable** configuration will not be displayed. When the Smartant function is disabled, the information on disabling configuration can be seen.
	`Ruijie(config)#show ap-config running ap320` `!` `ap-config ap320` `...` `...` `no smartant enable radio 2` `...` `...` `!`

6.5 Monitoring

Displaying

Description	Command
Displays AP configuration.	**show ap-config running** *ap-name*

7 Configuring FSS

7.1 Overview

By enabling frequency spectrum scanning (FSS), an AP can operate in the FSS mode and actually act as a wireless frequency spectrum sensor which is responsible for collecting and analyzing non-802.11 wireless signal frequency spectrum and sends the results of frequency spectrum analysis to the frequency spectrum analysis server. After processing, the frequency spectrum analysis server shows the results of frequency spectrum analysis to users in intuitive forms such as graphic, list and alarm.

FSS is used with Ruijie's SNC software to achieve frequency spectrum analysis.

7.2 Applications

Application	Description
Networking with the SNC Software to Achieve Frequency Spectrum Analysis	FSS is networked with Ruijie's SNC software to achieve frequency spectrum analysis.

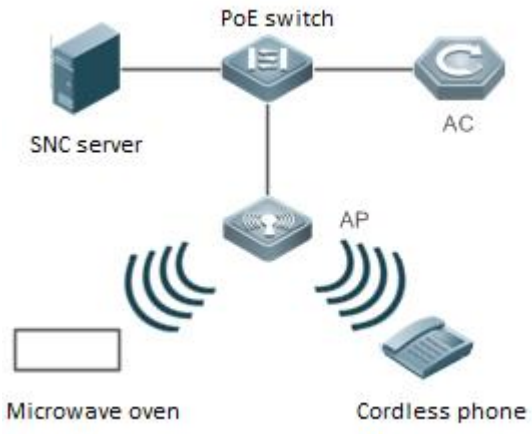
7.2.1 Networking with the SNC Software to Achieve Frequency Spectrum Analysis

Scenario

Ruijie's SNC software achieves frequency spectrum analysis. The SNC software is networked with Ruijie's wireless FIT AP system, as shown in Figure 7-1:

- There are non-802.11 wireless interference devices such as microwave ovens and cordless phones in the RF environment.

Figure 7-1



Remarks	A. The SNC software is installed on the SNC server. B. The AC and AP constitute the wireless FIT AP system.

	C. There are interferences from microwave ovens and cordless phones in the RF environment.

Deployment

- Enable frequency spectrum analysis on the AC.
- Establish a connection between the SNC software and the AC.

7.3 Features

Basic Concepts

Video Bridge Interference

During operation, a video bridge may generate wireless signals that interfere with WLAN transmission. The FSS of an AP can recognize and send the video bridge interferences to the SNC software for analysis.

Microwave Oven Interference

During operation, a microwave oven may generate microwave leakage that interferes with WLAN transmission. The FSS of an AP can recognize and send the microwave interferences to the SNC software for analysis.

Cordless Phone Interference

During operation, a cordless phone may generate wireless signals that interfere with WLAN transmission. The FSS of an AP can recognize and send the cordless phone interferences to the SNC software for analysis.

Bluetooth Interference

During operation, a Bluetooth device may generate wireless signals that interfere with WLAN transmission. The FSS of an AP can recognize and send the Bluetooth device interferences to the SNC software for analysis.

Continuous Wave

During operation, a continuous wave may generate wireless signals that interfere with WLAN transmission. The FSS of an AP can recognize and send the continuous wave interferences to the SNC software for analysis.

Scanning Precision

The scanning precision indicates the serial number of the scanned characteristic waveform which is then determined as a specific interference source. Normally, a higher scanning precision leads to a higher probability of correct determination.

Scanning Duration

When performing frequency spectrum scanning, an AP cannot provide normal wireless services. The system regularly switches between wireless services and frequency spectrum scanning to give consideration to both. A longer scanning duration leads to a higher probability of locating interferences.

Overview

Feature	Description

SNC Connecting to the AC for Frequency Spectrum Analysis	Through the interaction between SNC and AC, non-802.11 interference sources such as microwave ovens, cordless phones, and Bluetooth devices are recognized in a wireless environment.

7.3.1 SNC Connecting to the AC for Frequency Spectrum Analysis

An AP recognizes non-802.11 interference sources such as microwave ovens, cordless phones, and Bluetooth devices in a wireless environment and sends them to the SNC software for sort-out and display through the connection channel established between the AC and the SNC software.

Working Principle

Frequency spectrum analysis is achieved through the interaction and SOCKET connection between SNC and AC. After FSS is enabled, an AP regularly collects non-802.11 interference information in the RF environment and performs Fast Fourier Transform (FFT). Then the AP classifies the information for processing, recognizes and sends specific interference sources to the SNC software via the agreed protocol. After receiving information, the SNC software sorts out and displays the interference information in various ways. For specific operations, refer to Ruijie's user manual for the SNC software.

7.4 Configuration

Configuration	Description and Command	
Enabling FSS	⚠ (Mandatory) It is used to enable FSS.	
	spectral enable	Enables FSS.
Configuring the Interference Recognition Precision for Frequency Spectrum Scanning	⚠ (Optional) It is used to configure the interference recognition precision for frequency spectrum scanning.	
	spectral stability	Configures the interference recognition precision for frequency spectrum scanning.
Configuring the Frequency Spectrum Scanning Duration	⚠ (Optional) It is used to configure the frequency spectrum scanning duration.	
	spectral period	Configures the frequency spectrum scanning duration.

7.4.1 Enabling FSS

Configuration Effect

- Enable FSS.

Notes

- FSS is enabled in the AP configuration mode.

Configuration Steps

Enabling FSS

- (Mandatory) Run the **spectral enable** command to enable or disable FSS in the AP configuration mode.
- Enable FSS for the target AP that is FSS-capable in the AP configuration mode.

Command	**spectral enable**
Parameter Description	N/A
Defaults	FSS is disabled.
Command Mode	AP configuration mode
Usage Guide	-

Verification

Run the **show ap-config running** *ap-name* command to verify that the frequency spectrum scanning precision is configured on the target AP.

Configuration Example

Enabling FSS

Configuration Steps	● Enable FSS for a specified AP.
	Ruijie# configure terminal Ruijie(config)# ap-config AP0001 Ruijie(config-ap)# spectral enable Ruijie(config)# end
Verification	Run the **show ap-config running** *ap-name* command to verify that FSS is enabled on the target AP.
	Ruijie# show ap-config running AP0001 spectral enable

Common Errors

- This command is used in the all AP configuration mode.

7.4.2 Configuring the Interference Recognition Precision for Frequency Spectrum Scanning

Configuration Effect

- Configure the recognition precision of non-802.11 frequency spectrum signals where a larger value leads to a higher precision.

Notes

- FSS must be enabled.

Configuration Steps

Configuring the Interference Recognition Precision for Frequency Spectrum Scanning

- Optional
- The scanning precision is configured in the AP configuration mode, and the default value can be used.

Command	**spectral stability vbr** | **bth** | **bts** | **cph** | **mwo** | **cwa** *num*
Parameter Description	**vbr** *num*: configures the precision of video bridge recognition, ranging 1-5 and 5 by default. **bth** *num*: configures the precision of Bluetooth recognition, ranging 1-4 and 1 by default. **bts** *num*: configures the precision of Bluetooth earphone recognition, ranging 1-2 and 1 by default. **cph** *num*: configures the precision of cordless phone recognition, ranging 3-5 and 5 by default. **mwo** *num*: configures the precision of microwave recognition, ranging 1-5 and 1 by default. **cwa** *num*: configures the precision of continuous wave recognition, ranging 4-10 and 8 by default.
Defaults	See the parameter description.
Command Mode	AP configuration mode
Usage Guide	If there are no special requirements, the default value can be used.

Verification

Run the **show ap-config running** *ap-name* command to verify that the frequency spectrum scanning precision is configured on the target AP.

Configuration Example

Configuring the Frequency Spectrum Scanning Precision

Configuration Steps	• Configure the frequency spectrum scanning precision for video bridges as 2.
	`Ruijie# configure terminal` `Ruijie(config)# ap-config AP0001` `Ruijie(config-ap)# spectral enable` `Ruijie(config-ap)# spectral stability vbr 2` `Ruijie(config)# end`
Verification	Run the **show ap-config running** *ap-name* command to verify the frequency spectrum scanning precision on the target AP.
	`Ruijie# show ap-config running AP0001` `spectral enable` `spectral stability vbr 2`

Common Errors

- FSS is not enabled.
- This command is used in the all AP configuration mode.

7.4.3 Configuring the Frequency Spectrum Scanning Duration

Configuration Effect

- Change the duration required for one cycle of frequency spectrum scanning, 5 ms by default and ranging 1-100 ms.
- A longer scanning duration leads to a higher probability of locating interferences but a bigger influence on normal communication of the AP.

Notes

- FSS must be enabled.

↘ Configuring the Frequency Spectrum Scanning Duration

- Optional
- The scanning duration is configured in the AP configuration mode. If there are no special requirements, the default value can be used.

Command	**spectral period** *num*
Parameter Description	*num*: scanning duration, ranging 1-100 ms, 5 ms by default.
Defaults	5
Command Mode	AP configuration mode
Usage Guide	If there are no special requirements, the default value can be used.

Verification

Run the **show ap-config running** *ap-name* command to verify that the frequency spectrum scanning duration is configured on the target AP.

Configuration Example

↘ Configuring the Frequency Spectrum Scanning Duration as 10 μs

Configuration Steps	● Configure the frequency spectrum scanning duration as 10 μs.
	Ruijie# configure terminal Ruijie(config)# ap-config AP0001 Ruijie(config-ap)# spectral enable Ruijie(config-ap)# spectral period 10 Ruijie(config)# end

Verification	Run the **show ap-config running** *ap-name* command to verify the scanning duration configured on the target AP.
	`Ruijie# show ap-config running AP0001` `spectral enable` `spectral period 10`

Common Errors

- FSS is not enabled.
- This command is used in the all AP configuration mode.

8 Configuring Wireless Location

8.1 Overview

The Wireless Location (WL) function of Ruijie WLAN products uses 802.11 wireless signals to locate terminal stations (STAs). It is supported on all 802.11 a/b/g/n-compliant STAs, such as laptops, Mobile Units (MUs), and special Radio Frequency Identifications (RFIDs, hereinafter mainly referred to as TAGs). By analyzing and summarizing 802.11 wireless signals sent from these STAs, WL achieves STA locations through software on the location server in vivid forms such as maps, tables, or reports.

Ruijie WL also has the following characteristics:

- Support indoor and outdoor deployment.
- Support two algorithms, Received Signal Strength Indication (RSSI) location and Time Difference of Arrival (TDOA) location.
- Support two RFIDs, MUs and TAGs.

8.2 Applications

Application	Description
Centralized Location Deployment	Deploys the location system in fit AP mode.

8.2.1 Centralized Location Deployment

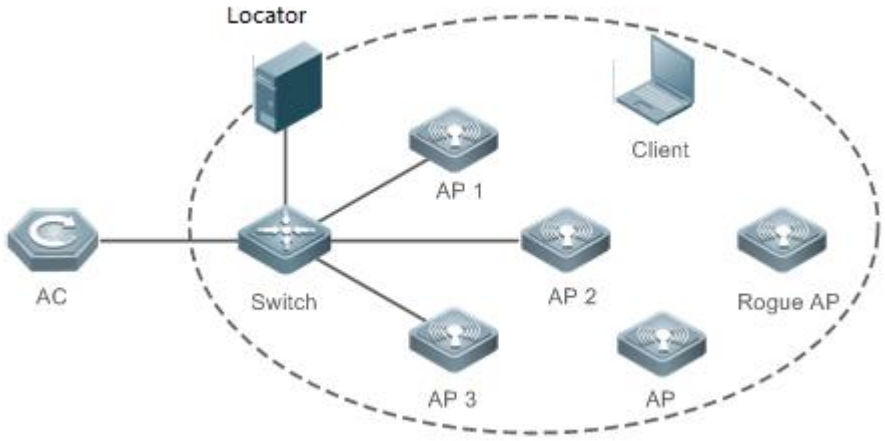
Scenario

Under WLAN in fit AP mode where Access Points (APs) are managed uniformly by the Access Controller (AC), the 802.11 STAs can be located by a Location Server or Locator. The special requirements are:

- Direct access is required between APs and the Locator. Therefore, make sure the ping between them is successful.
- The APs must be WL-capable Ruijie products.
- It is necessary to deploy three APs for accurate location.

The following figure is an example where AP 1, AP 2 and AP 3 can communicate with the Locator. Three APs respectively send received STA information to the Locator which then works out the STA locations.

Figure 8-1



Deployment

- The AC is responsible for WL configuration management and issuing.
- The APs are responsible for collecting STA information and sending the information as specified to the Locator.
- The Locator summarizes all the information sent from all APs, works out the STA locations, and displays the locations in maps or tables based on configurations by the administrator.

8.3 Features

Basic Concepts

A location system contains three parts: the Target or Source, the Receiver, and the Backend Location System.

Target or Source

Ruijie WL supports two types of location targets:

- TAGs, produced by AeroScout, a type of light and portable RFIDs which are usually placed or stuck on the targets to be located.
- MUs, 802.11-complicant wireless STAs regularly transmitting wireless signals.

Receiver

The Receiver can be a Ruijie AP or an AeroScout Tag exciter (used not to collect locations but to excite the TAGs to transmit specified wireless signals).

Backend Location System

The Backend Location System includes a Locator, AeroScout Engine (AE) computing software and all kinds of graphic programs.

Features

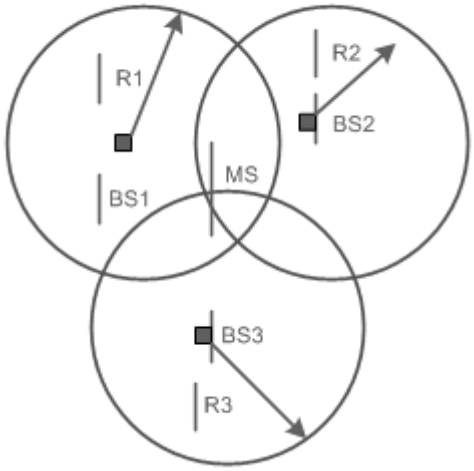
Feature	Description
WL	Enables WL for APs.

8.3.1 WL

Working Principle

Based on the measurement of RSSI from an MU received by a base station (BS) and the channel transmission model, the distance between them can be estimated to be d. In this way, for a BS (i), the MU must be on the circle centered at BS (i) with a radius of d. When three or more BSs are used for distance measurement of the same MU, the location of this MU can be determined. In this method, the main causes for location error are the multipath effect generated during signal transmission and the shadow effect generated during obstacle crossing. More accurate location can be achieved in open space without obstacles. However, in many circumstances, the location accuracy is significantly affected because of uncertainties, such as the multipath effect, attenuation, and scattering, due to various obstacles.

Figure 8-2



8.4 Configuration

Configuration	Description and Command	
Configuring WL Basic Features	(Mandatory) It is used to enable WL.	
	wlocation enable	Enables WL on a specified AP.
	wlocation ae-ip	Configures the IP address of the Locator connected to a specified AP.
	wlocation ae-port	Configures the port ID (PID) of the Locator connected to a specified AP.
	wlocation mu enable	Enables MU location on a specified AP.
	wlocation tag enable	Enables TAG location on a specified AP.
	(Optional) It is used to optimize the WL transmission.	
	wlocation compound enable	Enables the WL aggregation.
	wlocation send-mu-time	Configures the interval for sending MU location information on a specified AP.

Configuration	Description and Command	
	wlocation send-tag-time	Configures the interval for sending TAG location information on a specified AP.
	wlocation mu report enable	Enables WL location report.
	wlocation tag report enable	Enables TAG location report.
	wlocation mu report reduce enable	Simplifies MU location information.
	wlocation ignore beacon enable	Filters Beacon packets sent by APs.

8.4.1 Configuring WL Basic Features

Configuration Effect

- Enable WL to provide basic location services.

Notes

- N/A

Configuration Steps

Enabling WL on an AP

- Mandatory.
- Run the **wlocation enable** command to enable WL on an AP.
- Specify WL targets by running the **wlocation mu enable** and **wlocation tag enable** commands, which are used to enable WL for MUs and TAGs respectively.
- If WL is not enabled or no WL target is specified, WL cannot be used.
- Except as otherwise noted, enable WL for each AP in the deployment where location is required.

Command	**wlocation enable**
Parameter Description	N/A
Defaults	WL is disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the IP Address and PID for the Locator

- Mandatory.
- The PID is defaulted depending on the configuration of a specific Locator.
- The WL of APs works only with the Locator. Therefore, the IP address and PID of the Locator needs to be configured, guaranteeing its communication with the APs.
- The commands for configuring the IP address and PID are **wlocation ae-ip** *ip-address* and **wlocation ae-port** *port* respectively.

Command	**wlocation ae-ip** *ip-address*
Parameter	*ip-address*: IP address of the Locator

Description	
Defaults	No IP address is configured for the Locator. The AE server's default IP address is 0.0.0.0.
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**wlocation ae-port** *port*
Parameter Description	*port*: PID of the Locator
Defaults	The default PID is 12092.
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling MU or TAG Location

- Mandatory.
- To enable WL on an AP, you need to enable WL for MUs or TAGs. The configuration depends on the scenario and the STA to be located.

Command	**wlocation mu enable**
Parameter Description	N/A
Defaults	MU location is disabled.
Command Mode	AP configuration mode
Usage Guide	Both MU and TAG locations can be enabled at the same time.

Command	**wlocation tag enable**
Parameter Description	N/A
Defaults	TAG location is disabled.
Command Mode	AP configuration mode
Usage Guide	Both MU and TAG locations can be enabled at the same time.

Configuring the Interval for Sending MU or TAG Location Information

- Optional.
- It is used to adjust the interval for sending location information. Except as otherwise noted, the default value is applicable.
- In the scenarios with a lot of STAs to be located, reduce the interval to avoid information losses. (An AP can cache 500 to 700 pieces of location information.)

Command	**wlocation send-mu-time** *interval*

Parameter Description	*interval*: time interval, ranging from 100 to 5,000 ms
Defaults	The default interval is 300 ms.
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**wlocation send-tag-time** *interval*
Parameter Description	*interval*: time interval, ranging from 100 to 5,000 ms
Defaults	The default interval is 300 ms.
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling MU Location Report

- Optional.
- The Locator does not intercommunicate with APs which directly send collected MU location information, for example, through the NAT network. Except as otherwise noted, the default value is applicable.

Command	**wlocation mu report enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	With this function enabled, the handshake process of the protocol (referring to the private protocol provided by Aeroscout itself for intercommunication between the Locator and APs) is ignored except through the NAT.

Enabling TAG Location Report

- Optional.
- The Locator does not intercommunicate with APs which directly send collected TAG location information, for example, through the NAT network. Except as otherwise noted, the default value is applicable.

Command	**wlocation tag report enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	With this function enabled, the handshake process of the protocol (referring to the private protocol provided by Aeroscout itself for intercommunication between the Locator and APs) is ignored except through the NAT.

Simplifying MU Location Information

- Optional.
- Use this command where there is a requirement for lower traffic bandwidth, and the deployed location system interconnects with the location server developed by Ruijie Networks. Except as otherwise noted, you can apply the configuration on your demand.

Command	wlocation mu report reduce enable
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Enable the function of simplifying MU location information to reduce bandwidth traffic, which applies only when the deployed location server is developed by Ruijie Networks.

Filtering Beacon Packets Sent by APs

- Optional.
- Use this command where there is a requirement for traffic bandwidth reduction. Except as otherwise noted, you can apply the configuration on your demand.

Command	wlocation ignore beacon enable
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Enable the function of filtering Beacon packets sent by APs in Wi-Fi environment to reduce bandwidth traffic.

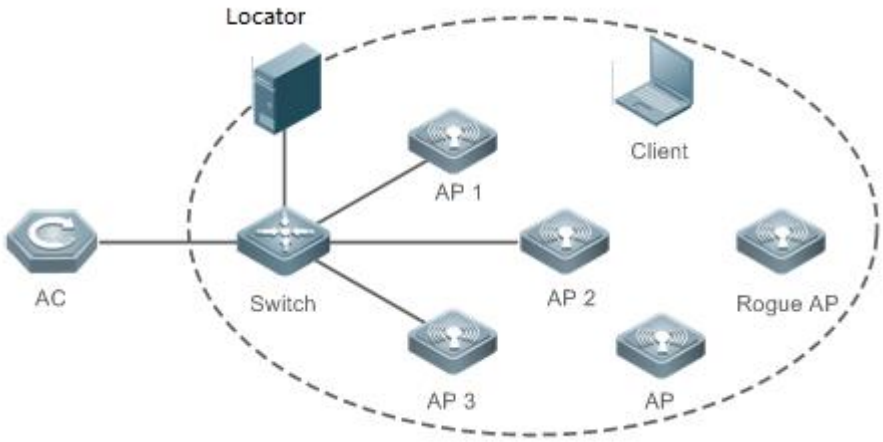
Verification

In the deployed network, enable STAs to send wireless packets.

- Verify that APs receive wireless location information.
- Verify that the Locator receives location information.

Configuration Example

Enabling WL

Scenario **Figure 8-3**	
Configuration Steps	● Enable WL. ● Configure the IP address of the Locator. ● Enable MU location as required. ● Enable TAG location as required. ● Assuming that AP1 in the above figure is named ap1-1, run the following commands to enable ML for this AP.
AP1	`Ruijie# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)# ap-config ap1-1` `Ruijie(ap-config)# wlocation enable` `Ruijie(ap-config)# wlocation ae-ip 1.1.1.1` `Ruijie(ap-config)# wlocation mu enable` `Ruijie(ap-config)# wlocation tag enable`
Verification	● Run the **show ap-config** command to display the configurations of each AP and verify ML configuration. ● Assuming that AP1 in the above figure is named ap1-1, run the following commands to verify the ML configuration for this AP.
AP1	`AC5302_7#show ap-config running` `ap-config ap1-1` `wlocation enable` `wlocation ae-ip 1.1.1.1` `wlocation mu enable` `wlocation tag enable`

Common Errors

N/A

9 Configuring RRM 2.0

9.1 Overview

Radio resource management (RRM) is an important function on the AC for managing RF resources of APs.

The RRM analyzes peripheral RF environments and adjusts the RF channel and power of APs based on specific algorithms to prevent signal interference between APs and ensure proper running of the wireless network.

When an AP has strong interference due to a complex RF environment, enabling the RRM function can improve user experience.

9.2 Features

Basic Concepts

STA, AP, and AC

- STA: wireless stations with wireless network interface cards (NICs), for example, laptops and mobile phones
- AP: wireless access point that provides wireless signal access for STAs
- AC: wireless access controller that manages APs and provides wireless network services

RF Environment Information

- STA information: includes the received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) of STAs.
- Neighbor information: includes the RSSI and working channels of neighboring APs.
- Noise: indicates the noise value that affects 802.11 signal receiving, in dBm.
- Interference(%): includes 802.11 signal interference and non-802.11 signal interference. The former indicates signal interference from other APs, and the latter indicates interference from microwave ovens and Bluetooth devices.

Co-channel Interference

When two closely deployed APs work in the same channel, co-channel interference occurs, affecting 802.11 wireless packet receiving.

Overview

Feature	Description
Channel Adjustment	Based on the peripheral RF environment, the AC allocates a proper working channel for an AP to reduce the co-channel interference and improve the wireless access experience of users.
Power Control	When APs are closely deployed and the TX power of an AP is high, the rest APs may be affected. Therefore, the TX power of the AP needs to be lowered to reduce interference.

To perform RRM 2.0 channel adjustment and power control, APs need to support RRM 1.0 or RRM 2.0. Channel adjustment and power control are supported for APs that support RRM 1.0 after they interwork with ACs that support RRM 2.0. However, scanning results reported by APs are limited. When multiple interference signals exist (for example, interference from private APs), the adjustment effect is not optimal.

To display RRM versions supported by online APs, run the **show rrm support** command on the AC.

9.2.1 Channel Adjustment

From a perspective of an AP, channel adjustment prevents the AP from serious interference in the working channel.

From a perspective of the global RF environment, proper channel allocation to each AP ensures the minimum interference between APs and improves the spectrum resource utilization and user experience.

Working Principle

When two closely deployed APs work in the same channel, a wireless signal conflict or interference occurs, affecting wireless user experience.

The ADCA algorithm comprehensively analyzes various environment factors and allocates the optimal working channels for all APs, preventing channel conflicts.

For example, if two APs work in the same channel or two channels with overlapped spectrum resources, the ADCA algorithm will stagger their channels to optimize spectrum resources.

9.2.2 Power Control

Power control is used to lower the TX power of an AP to reduce signal interference between APs.

Working Principle

When an AP is powered on for the first time, it uses the allowed maximum TX power according to national or regional regulations. Higher TX power indicates larger signal coverage. If signal coverage of adjacent APs overlaps and the APs are in the same frequency band, strong co-channel interference exists. The ATPC algorithm determines whether to raise or lower the TX power of an AP based on neighbor information of the AP. When co-channel interference between APs is strong and channels cannot be staggered, the TX power of APs has to be lowered to reduce co-channel interference. If there is no co-channel interference between APs, raise the TX power to expand the signal coverage area.

If channel adjustment and power control are enabled simultaneously, RRM 2.0 preferentially adjusts the channel and then the power. If channels can be staggered, the TX power does not need to be lowered. For this purpose, the ATPC algorithm is executed after the ADCA algorithm.

9.3 Configuration

Configuration	Description and Command	
Configuring Channel Adjustment	(Optional) It is used to configure parameters related to channel adjustment.	
	rrm [**2.4g** | **5g**] **mode enable**	Enables automatic RF adjustment for newly deployed APs.
	rrm [**2.4g | 5g**] **channel dynamic enable**	Enables dynamic channel adjustment.
	rrm [**2.4g | 5g**] **channel bandwidth {current | optimal}**	Selects the channel bandwidth policy during channel adjustment.
	rrm [**2.4g | 5g**] **update channel**	Manually enables channel planning.
	rrm [**2.4g | 5g**] **appoint** *date time*	Reserves a time to adjust the channel and power for all online APs.
Configuring Power Control	(Optional) It is used to configure parameters related to power control.	
	rrm [**2.4g** | **5g**] **mode enable**	Enables automatic RF adjustment for newly deployed APs.
	rrm [**2.4g | 5g**] **update txpower**	Manually enables power planning.
	rrm [**2.4g | 5g**] **appoint** *date time*	Reserves a time to adjust the channel and power for all online APs.

9.3.1 Configuring Channel Adjustment

Configuration Effect

- After channel adjustment is enabled, the AC allocates proper working channels for APs based on their RF environments to improve the wireless network experience.

Configuration Steps

Configuring Channel Adjustment

- Optional. To enable the AC to allocate proper working channels for APs, configure the channel adjustment function.
- Run the **rrm** [**2.4g** | **5g**] **mode enable** command to enable automatic channel adjustment for newly deployed APs.
- Run the **rrm** [**2.4g | 5g**] **channel bandwidth {current | optimal}** command to configure the channel bandwidth policy.
- Run the **rrm** [**2.4g** | **5g**] **channel dynamic enable** command to enable dynamic channel adjustment.
- Run the **rrm** [**2.4g** | **5g**] **update channel** command to manually enable channel planning.
- Run the **rrm** [**2.4g** | **5g**] **appoint** *date time* command to reserve a time to adjust the channel and power for all online APs.

Command	**rrm** [**2.4g** | **5g**] **mode enable**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network
Defaults	Automatic channel adjustment is disabled for newly deployed APs on the 2.4 GHz and 5 GHz networks by default.

Command Mode	Global configuration mode
Usage Guide	When a newly deployed AP goes online, RF adjustment is performed for the AP. Original configuration is retained for existing APs when they go online. The channel and power of newly deployed APs in the same frequency band are adjusted simultaneously.

Command	**rrm** [**2.4g** | **5g**] **channel bandwidth {current | optimal}**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network **current**: The current channel bandwidth configuration is selected during channel planning. **optimal**: The optimal channel bandwidth configuration is selected automatically during channel planning.
Defaults	The optimal channel bandwidth policy is configured for the 2.4 GHz and 5 GHz networks by default.
Command Mode	Global configuration mode
Usage Guide	The optimal policy automatically selects the channel bandwidth configuration based on different radio types of APs and channel limitation of radios. The selection rules are as follows: (1) Use HT20 for the 2.4 GHz frequency band. (2) Use HT40 for the 5 GHz frequency band without channel limitations. (3) Use HT40 for radios that are limited to channels 36 to 64. (4) Use HT20 for radios that are limited to channels 149 to 165.

Command	**rrm** [**2.4g** | **5g**] **channel dynamic enable**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network
Defaults	Dynamic channel adjustment is disabled for the 2.4 GHz and 5 GHz networks by default.
Command Mode	Global configuration mode
Usage Guide	When dynamic channel adjustment is enabled, RRM 2.0 checks channel interference of APs every 5 minutes. If the channel interference exceeds the threshold, RRM 2.0 triggers channel adjustment for the APs. Adjusted channel configuration will overwrite original channel and channel bandwidth configuration (the optimal policy is selected) of APs in ap-config mode. In addition, STAs may be kicked offline due to channel switch during adjustment.

Command	**rrm** [**2.4g** | **5g**] **update channel**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	After adjustment is completed, automatic RF adjustment is enabled for newly deployed APs in the corresponding frequency band automatically.

Command	**rrm** [**2.4g** | **5g**] **appoint** *date time*
Parameter	**2.4g**: 2.4 GHz network

Description	**5g**: 5 GHz network *date*: reservation date, in the format of yyyy-MM-dd *time*: reservation time, in the format of hh:mm:ss
Defaults	No reservation time is set by default.
Command Mode	Global configuration mode
Usage Guide	The channel and power of online APs will be adjusted simultaneously at the reserved time. After adjustment is completed, automatic RF adjustment is enabled for newly deployed APs in the corresponding frequency band automatically.

Verification

- Run the **show rrm** [**2.4g** | **5g**] **summary** command to display the channel adjustment status.
- Run the **show ap-config summary** command to display the channel adjustment results of APs.

Configuration Example

Configuring Channel Adjustment Parameters

Configuration Steps	Enable automatic channel planning for newly deployed APs.
AC	`AC#configure terminal` `AC(config)#rrm mode enable` `AC(config)#exit`
Verification	Display the channel adjustment status.
AC	`Ruijie#show rrm 2.4g summary` `Radio Resource Management` `  Radio Type..... 2.4G` `  RRM Enable Mode..... Enable` `  Channel Width Strategy..... Optimal` `  Channel Dynamic Enable Mode..... Enable` `  Run Status..... Finish`

9.3.2 Configuring Power Control

Configuration Effect

- After power control is enabled, the AC configures proper TX power for APs based on their RF environments to reduce co-channel interference between the APs.

Notes

- Power control is used to reduce co-channel interference of an AP to other APs. The ATPC algorithm needs to obtain the co-channel interference from other APs to determine whether to control the power. Currently, power control is supported among multiple Ruijie APs.

Configuration Steps

↘ Configuring Power Control

- Optional. To control APs' TX power to prevent co-channel interference between APs, configure the power control function.
- Run the **rrm** [**2.4g** | **5g**] **mode enable** command to enable automatic power adjustment for newly deployed APs.
- Run the **rrm** [**2.4g** | **5g**] **update txpower** command to manually enable power adjustment.
- Run the **rrm** [**2.4g** | **5g**] **appoint** *date time* command to reserve a time to adjust the channel and power for network-wide online APs.

Command	**rrm** [**2.4g**	**5g**] **mode enable**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network
Defaults	Automatic power adjustment is disabled for newly deployed APs on the 2.4 GHz and 5 GHz networks by default.
Command Mode	Global configuration mode
Usage Guide	When a newly deployed AP goes online, RF adjustment is performed for the AP. Original configuration is retained for existing APs when they go online. The channel and power of newly deployed APs in the same frequency band are adjusted simultaneously.

Command	**rrm** [**2.4g**	**5g**] **update txpower**
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**rrm** [**2.4g**	**5g**] **appoint** *date time*
Parameter Description	**2.4g**: 2.4 GHz network **5g**: 5 GHz network *date*: reservation date, in the format of yyyy-MM-dd *time*: reservation time, in the format of hh:mm:ss
Defaults	No reservation time is set by default.
Command Mode	Global configuration mode
Usage Guide	The channel and power of online APs will be adjusted simultaneously at the reserved time.

Verification

- Run the **show rrm** [**2.4g** | **5g**] **summary** command to display the power adjustment status.
- Run the **show ap-config summary** command to display the channel adjustment results of APs.

Configuration Example

Configuring Power Control Parameters

Configuration Steps	Enable the power adjustment function.
AC	`AC#configure terminal` `AC(config)#rrm mode enable` `AC(config)#exit`
Verification	Display the power control status.
AC	`Ruijie#show rrm 2.4g summary` `Radio Resource Management` `Radio Type..... 2.4G` `RRM Enable Mode..... Enable` `Channel Width Strategy..... Optimal` `Channel Dynamic Enable Mode..... Enable` `Run Status..... Finish`

9.4 Monitoring

Displaying

Description	Command
Displays basic RRM configuration.	**show rrm** [**2.4g** | **5g**] **summary**
Displays RRM versions supported by online APs.	**show rrm support**

10 Configuring 802.11kv

10.1 Overview

The 802.11k protocol revises radio resource measurement (RRM) of the 802.11 protocol, which enables APs and STAs to obtain the RRM data of each other. The 802.11v protocol revised wireless network management (WNM) of the 802.11 protocol. The 802.11k/802.11v protocol enables ACs to manage wireless network resources better and supports the load balancing function. This document describes the application scenarios and configuration methods for channel utilization balancing and STA quantity balancing between radios.

Protocols and Standards

- IEEE 802.11k-2008: Amendment 1: Radio Resource Measurement of Wireless LANs
- IEEE 802.11v-2011: Amendment 8: IEEE 802.11 Wireless Network Management

10.2 Applications

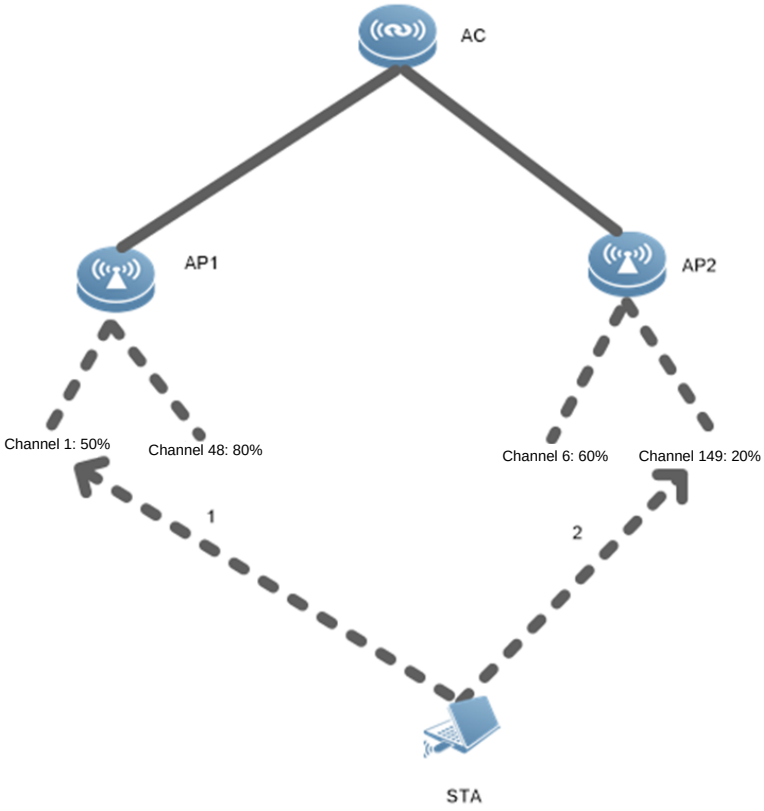
Application	Description
Channel Utilization Balancing	Fit AP networking is adopted, including at least one AC and two APs.
STA Quantity Balancing Between Radios	Fit AP networking is adopted, including at least one AC and two APs.

10.2.1 Channel Utilization Balancing

Scenarios

On a wireless network, especially in high-density STA deployment scenarios, channel utilization is unbalanced due to various reasons. Because STAs cannot perceive the channel utilization, they may select a channel with the highest utilization. Therefore, channel utilization balancing is required to migrate STAs to channels with low utilization within 2s to 10s after STAs go online, to improve user experience.

Figure 10-1



Remarks	AC: wireless access controller AP: wireless access point STA: terminal

Deployment

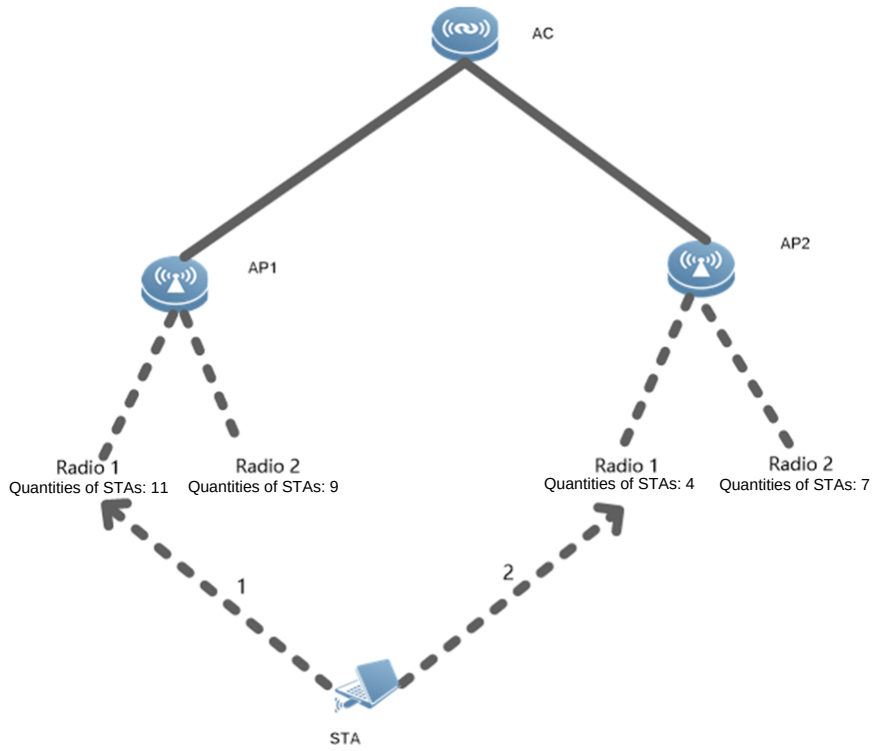
- Set the load balancing mode to channel utilization balancing on the AC.
- Set load balancing parameters on the AC.

10.2.2 STA Quantity Balancing Between Radios

Scenarios

When APs are deployed densely, multiple STAs may connect to the same AP. As a result, the STA quantities on APs are unbalanced.

Figure 10-2



Remarks	AC: wireless access controller AP: wireless access point STA: terminal

Deployment

- Set the load balancing mode to STA quantity balancing between radios on the AC.
- Set parameters of STA quantity balancing between radios on the AC.

10.3 Features

Basic Concepts

Channel Utilization

Channel utilization is an important indicator that affects the STA connection quality. When the traffic is heavy, the quantity of connected STAs is large, or interference is strong, the channel utilization is high. When a STA connects to an SSID that contains multiple BSSIDs, the STA will select a BSSID with the strongest signals. However, the BSSID with the strongest signals may have high channel utilization.

Minimum Load Balancing Value

A minimum value is required to trigger load balancing.

Load Balancing Gain Value

Load balancing is used to obtain better connection quality. If the connection quality and other indicators are not changed or changed slightly after load balancing is enabled, load balancing makes no sense. Therefore, a gain value, namely, a difference value, needs to be set, to determine an improvement produced after a STA is migrated to a radio or channel.

Overview

Feature	Description
Load Balancing	Improves the STA connection quality and balances AP load.

10.3.1 Load Balancing

Load balancing ensures that STAs are evenly distributed on channels or radios to obtain better connection experience.

Working Principle

When a STA that supports the 802.11k protocol is associated with the AC, the AC can obtain the list of available BSSIDs of the STA in real time. Each BSSID corresponds to one value (dBm). If the STA does not support the 802.11k protocol, the AC obtains the list of available BSSIDs of the STA through the probe frame. Load balancing is performed as follows after being enabled:

If a STA is on a channel with 70% or higher utilization, the STA can be migrated to a BSSID with channel utilization 20% less than the current channel and with highest signal strength that is no less than –63 dBm.

If a STA is on a radio with 10 or more connected STAs, the STA can be migrated to a BSSID with 5 STAs less and with highest signal strength that is no less than –63 dBm.

10.4 Configuration

Configuration	Description and Command	
Enabling 802.11k/802.11v	(Optional) It is used to set the policy template.	
	802.11kv enable	Enables the 802.11k/802.11v protocol.
Configuring the load balancing mode	(Mandatory) It is used to set the load balancing mode.	
	802.11kv load-balance mode channel-utilization	Sets the load balancing mode to channel utilization balancing.
	802.11kv load-balance mode station-number	Sets the load balancing mode to STA quantity balancing between radios.
	802.11kv load-balance mode none	Disables load balancing.

10.4.1 Configuring Channel Utilization Balancing

Configuration Effect

- When a STA that supports the 802.11v protocol is associated with a channel with utilization higher than the preset value, and another channel with lower utilization is available (the difference value is lower than the preset gain value), the STA will be migrated to the available channel.

Notes

Load balancing takes effect only to STAs that support 802.11k and 802.11v.

If most STAs do not support 802.11k, run the **sticky-steering enable** command in the ap-group configuration mode. This command is used to learn probe frames sent before a STA is associated, to determine the STA location. However, the command cannot be used to determine the STA location in real time as in 802.11k and is only supported in VAC scenarios.

Configuration Steps

- Mandatory.
- Run the **802.11kv enable** command in global configuration mode on the AC.

Command	802.11kv enable
Parameter Description	N/A
Defaults	802.11k/802.11v is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Setting the Load Balancing Mode

- Mandatory.
- Run the **802.11kv load-balance mode** command in global configuration mode on the AC.

Command	**802.11kv load-balance mode channel-utilization**
Parameter Description	N/A
Defaults	By default, load balancing is not performed.
Command Mode	Global configuration mode
Usage Guide	Channel utilization balancing is triggered when a STA is associated with a channel with utilization equal to or greater than 70% and there are neighboring channels with utilization 20% less than the associated channel.

Verification

- Run the **show running** command to display information based on the policy template and WLAN association information.

10.4.2 Configuring STA Quantity Balancing Between Radios

Configuration Effect

When a STA is associated with a radio on which the quantity of connected STAs is greater than or equal to the preset limit value and there is a neighboring radio on which the quantity of connected STAs is less than the preset limit value, the STA will be migrated to the neighboring radio.

Notes

Load balancing takes effect only to STAs that support 802.11k and 802.11v.

Configuration Steps

Enabling 802.11k/802.11v

- Mandatory.
- Run the **802.11kv enable** command in global configuration mode on the AC.

Command	802.11kv enable
Parameter Description	N/A
Defaults	802.11k/802.11v is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the Load Balancing Mode

- Mandatory.
- Run the **802.11kv load-balance mode** command in global configuration mode on the AC.

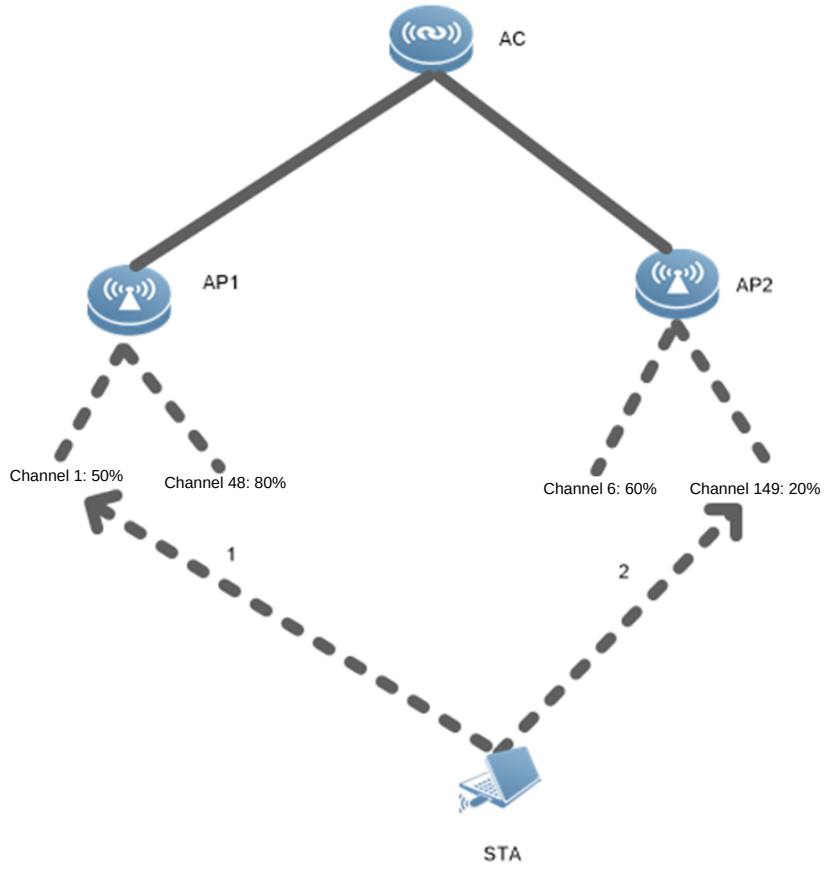
Command	**802.11kv load-balance mode station-number**
Parameter Description	N/A
Defaults	By default, load balancing is not performed.
Command Mode	Global configuration mode
Usage Guide	STA quantity balancing between radios is triggered when a STA is associated with a radio on which the quantity of connected STAs is greater than 10 and there is a neighboring radio on which the quantity of connected STAs is 5 STAs less.

Verification

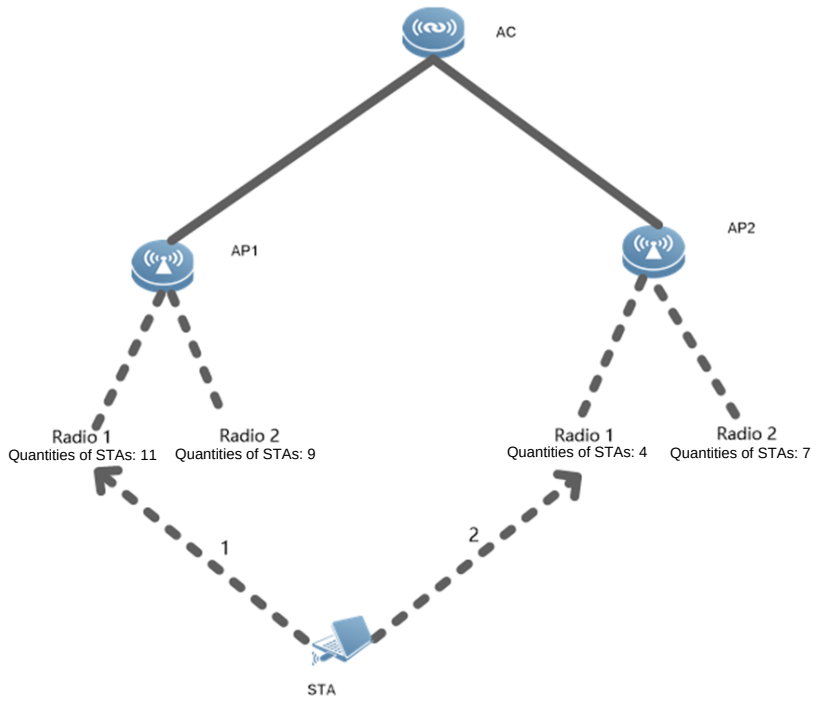
Run the **show running** command to display information based on the policy template and WLAN association information.

Configuration Example

Configuring Channel Utilization Balancing

Scenario **Figure 10-3**	
Configuration Steps	Enable 802.11k/802.11v.
AC	`Ruijie(config)802.11kv enable`
	Set the load balancing mode.
	`Ruijie(config)#802.11kv load-balance mode channel-utilization`
Verification	Run the **show run** command to display configuration information.
AC	`Ruijie#show run | begin 802.11kv` `802.11kv enable` `802.11kv load-balance mode channel-utilization`

↘ **Configuring STA Quantity Balancing Between Radios**

Scenario **Figure 10-4**	
Configuration Steps	Enable 802.11k/802.11v.
AC	`Ruijie(config)802.11kv enable`
	Set the load balancing mode.
	`Ruijie(config)# 802.11kv load-balance mode station-number`
Verification	Run the **show run** command to display configuration information.
AC	`Ruijie#show run | begin 802.11kv` `802.11kv enable` `802.11kv load-balance mode station-number`

10.5 Monitoring

Displaying

Description	Command
Displays BSTM records sent by the AC to all STAs.	**show 802.11kv all-bstms**
Displays BSTM records sent by the AC to a specific STA.	**show 802.11kv bstms-per-station**

WLAN Security Configuration

1. Configuring Robust Security Network Architecture
2. Configuring WIDS
3. Configuring CPU Protect Policy
4. Configuring NFPP
5. Configuring WAPI

1 Configuring Robust Security Network Architecture

1.1 Overview

The Robust Security Network Architecture (RSNA) function provides security mechanisms for WLANs.

A WLAN uses open media and public electromagnetic waves as a carrier to transmit data signals. Neither communication party is connected with a cable. If transmission links are not properly protected through encryption, data transmission will be at great risk. <Therefore, security mechanisms are especially important in a WLAN.

To enhance the security, a WLAN should be provided with at least the authentication and encryption mechanisms:

- Authentication mechanism: The authentication mechanism is used to authenticate users and allow only specified users (authorized users) to use network resources.
- Encryption mechanism: The encryption mechanism is used to encrypt data on wireless links to ensure that WLAN data can be received and understood only by expected users.

Protocols and Standards

- IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard -Aug 2004
- Information technology – Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements – 802.11, 1999 IEEE Standard for Local and metropolitan area networks ”Port-Based Network Access Control” 802.1X™ -2004
- 802.11i IEEE Standard for Information technology –Telecommunications and information exchange between systems –Local and metropolitan area networks – Specific requirements

1.2 Applications

Application	Description
WEP Encryption	In a small WLAN that has a lower requirement for security, static WEP encryption can be used to protect wireless data communication.
PSK Access Authentication	For small and medium-sized enterprise networks or family users, access authentication based on pre-shared keys can be used to enhance the security of WLANs.
802.1X Access Authentication	For a scenario that has a higher requirement for security or unified management, port-based network access control can be used.
802.11r	The fast roaming mode Fast BSS Transition (FT) is defined to reduce network delay caused by roaming.

WPA3 Authentication	WPA3 is a wireless authentication security standard released by Wi-Fi Alliance in 2018. Compared with WPA2, it is greatly improved in security.

1.2.1 WEP Encryption

Scenario

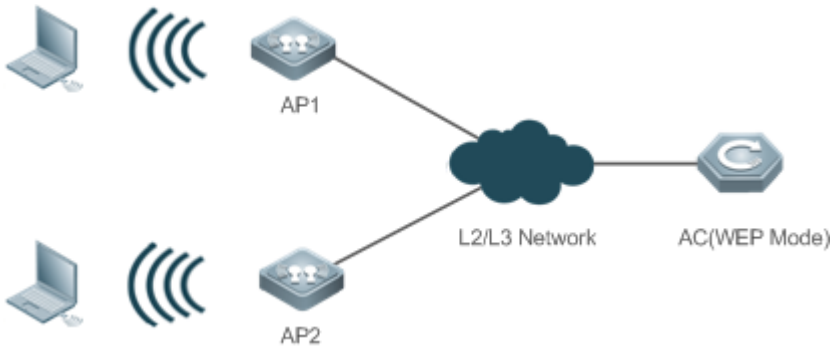
In a small WLAN that has a lower requirement for security, WEP encryption can be used.

WEP encryption can use the open-system or shared-key link authentication mode. Their differences are as follows:

- When open-system link authentication is used, WEP keys can be used only for data encryption. Even if inconsistent keys are configured, users can go online; however, data transmitted after the users go online is discarded by the receiver due to key inconsistency.
- When shared-key link authentication is used, WEP keys are used for link authentication and data encryption. If inconsistent keys are configured, link authentication fails and the client cannot go online.

Figure 1-1 shows the scenario of static WEP encryption.

Figure 1-1



Deployment

- Configure a WLAN on the AC.
- Configure WEP encryption in WLAN security configuration mode.
- Push the WLAN to APs.

1.2.2 PSK Access Authentication

Scenario

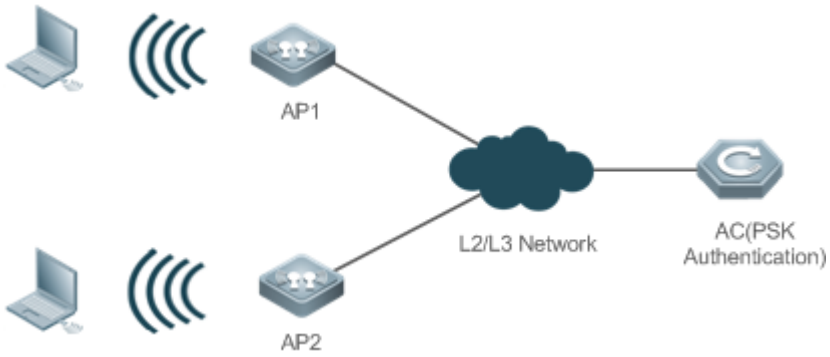
Small and medium-sized enterprise networks or family users can use the WPA or WPA2 standard to enhance WLAN security. The simplest method is to use the pre-shared key authentication (referred to as WPA-PSK and WPA2-PSK respectively). In this case, WPA is similar to WEP, but users can achieve higher security through WPA and 802.11i, including more robust authentication and better encryption algorithms.

In PSK authentication, the same pre-shared key should be configured for an STA and an AP to establish connection and

communication. No additional authentication server is required.

Figure 1-2 shows the scenario of PSK authentication.

Figure 1-2



Deployment

- Configure a WLAN on the AC.
- Configure PSK authentication in WLAN security configuration mode.
- Push the WLAN to APs.
- Use this authentication with WEB authentication to support web-based authentication and charging.

1.2.3 802.1X Access Authentication

Scenario

In a scenario that has a higher requirement for security, 802.1X authentication can be used.

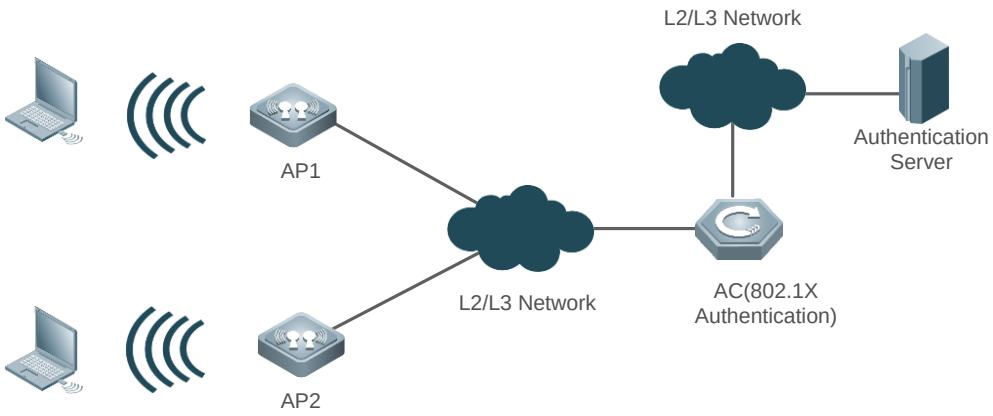
802.1X is a port-based network access control protocol. This authentication mode is used to authenticate and control STAs at the port level. STAs connected to the ports can access a WLAN if they pass the authentication; otherwise, the STAs fail to access the WLAN.

Authentication client software needs to be installed on terminals to perform 802.1X authentication. However, in some cases, some devices cannot be installed with the software, for example, wireless printers. For the sake of network management and security, although these terminals have no 802.1X authentication client software, administrators need to control the access of these terminals. MAC Authentication Bypass (MAB) provides a solution for this application.

After the MAB function is deployed for a WLAN, a wireless device can automatically probe the MAC address of a connected terminal and uses the MAC address to initiate a request to the authentication server.

Figure 1-3 shows the scenario of 802.1X authentication.

Figure 1-3



Deployment

- Configure a WLAN on the AC.
- Configure an authentication server on the AC.
- Configure 802.1X authentication in WLAN security configuration mode.
- Push the WLAN to APs.

1.2.4 802.11r

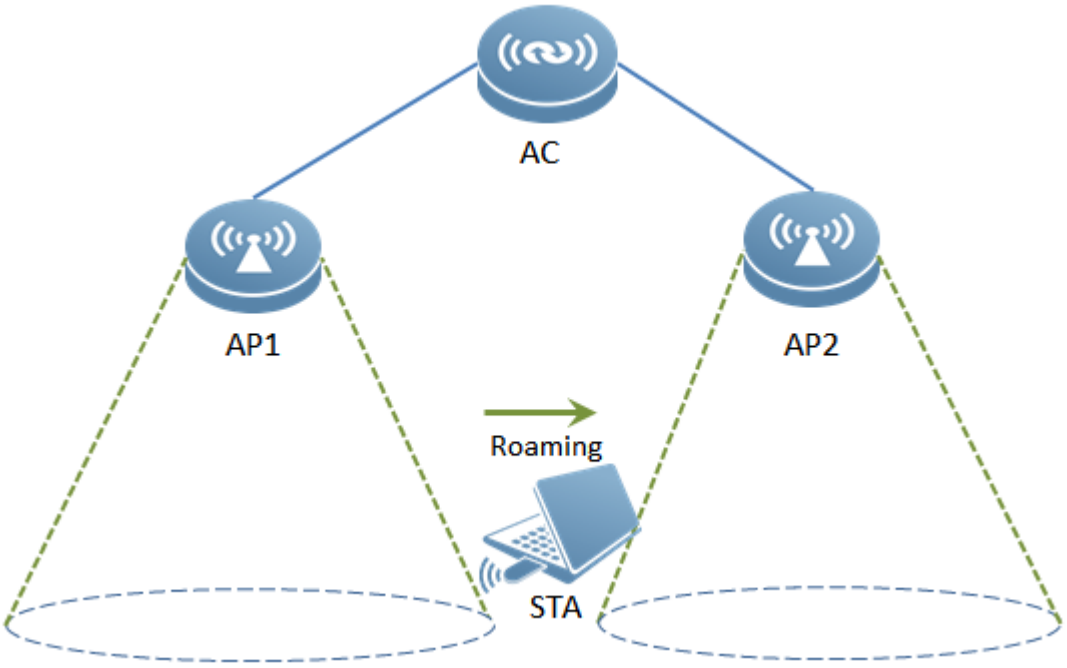
Scenario

For applications that are sensitive to network delay, such as voice over Wi-Fi and video, reducing the roaming authentication time is very important. The 802.11r standard defines the FT roaming mode. In this mode, 802.1x authentication and the 4-way handshake are not required, thereby reducing the roaming handover time.

The FT roaming mode includes the Over the Air and Over the DS methods. Currently, only Over the Air is supported. In this mode, STAs directly connect to a new AP for authentication in roaming scenarios.

The following figure shows the Over the Air application scenario.

Figure 1-4



Deployment

- Configure a WLAN on the AC.
- In WLAN security configuration mode, set authentication mode to RSN, access authentication mode (AKM) to PSK or 802.1x, and encryption mode to AES.
- Deliver the WLAN configuration to APs.
- Simulate a scenario in which an STA roams from AP1 to AP2. If the 802.11r function is enabled, the STA directly connects to AP2 for FT authentication.

1.2.5 WPA3 Authentication

Scenario

Wi-Fi Alliance released the Wi-Fi Protected Access III (WPA3) standard in 2018. This new standard supports three modes: WPA3 Personal, WPA3 Enterprise, and WPA3 Enhanced-Open.

The WPA3 Personal mode is similar to the Pre-shared Key (PSK) mode of WPA2 but the difference is that the Simultaneous Authentication of Equals (SAE) exchange is added in the phase of authentication using management packets. Therefore, the subsequent 4-way handshake no longer uses simple Pairwise Master Keys (PMKs) derived from passwords and it is impossible to intercept 4-way handshake packets to initiate dictionary attacks and crack passwords. Security is greatly enhanced in this mode.

The WPA3 Enterprise mode is similar to the 802.1x authentication of WPA2 but the 4-way handshake uses an updated cipher suite, which raises the overall security from 128-bit encryption to 192-bit encryption. In WPA3 Enterprise mode, security is significantly improved.

In WPA3 Enhanced-Open mode, users do not need to enter authentication information, interactive packets between STAs and APs are encrypted to prevent packet from eavesdropping. It is strong in privacy protection.

Deployment

- Configure a WLAN on an AC.
- Select the WPA3 mode in WLAN security mode.
- Deliver WLAN configuration to APs.

1.3 Features

Basic Concepts

WPA

Wi-Fi Protected Access (WPA) is a wireless security draft defined by the Wi-Fi Alliance. The IEEE802.11i standard is compatible with this draft.

RSN

The IEEE802.11i standard defines the concept of Robust Security Network (RSN): and makes many improvements against various defects of the WEP encryption mechanism. The functions are equal to WPA2 launched by the Wi-Fi Alliance.

TKIP

The Temporal Key Integrity Protocol (TKIP) is an enhancement on WEP security. TKIP provides key mixing, message integrity check and key mechanism re-generation for each packet, thus eliminating hidden risks of WEP.

AES

Advanced Encryption Standard (AES) is a new encryption standard published by the National Institute of Standards and Technology (NIST) of the United States. On October 2, 2000, the Rijndael algorithm designed by Joan Daemen and Vincent Rijmen from Belgium won with its excellent performance and anti-attack capabilities, and became the new-generation encryption standard AES.

CCMP

Counter CBC-MAC Protocol (CCMP) uses AES, which is safer than TKIP.

AKM

Authentication and Key Management (AKM) is an access authentication mode for users to access a WLAN.

SAE

Simultaneous Authentication of Equals (SAE) is a peer authentication interaction, which uses elliptic curve cryptography.

OWE

Opportunistic Wireless Encryption (OWE) does not need users to enter authentication information, and STAs and APs negotiate temporary PMKs.

Overview

Feature	Description
Link Verification	Verify the security of a wireless link before an STA associates with a WLAN.
Access Authentication	Perform authentication for an STA that accesses a WLAN.
Wireless Data Encryption	Implement security protection for communication data of an STA that accesses a WLAN.

1.3.1 Link Verification

Link verification refers to 802.11 authentication, which is a low-level authentication mechanism. Link verification is performed when an STA associates with an AP over 802.11, which is earlier than access authentication. Before accessing a WLAN, the STA must be authenticated over 802.11. 802.11 authentication marks the beginning of the handshake process when an STA accesses a WLAN and the first step for network connection.

The IEEE 802.11 standard defines two approaches to link authentication:

- Open-system link authentication
- Shared-key link authentication

Working Principle

↘ Open-System Link Authentication

Open-system link authentication allows all users to access a WLAN. In this sense, no data protection is provided, which means that no authentication is performed. In other words, if the authentication mode is set to open-system authentication, all STAs that request authentication can pass the authentication.

Open-system link authentication comprises two steps:

Step 1: An STA requests authentication. The STA sends an authentication request that contains the ID (usually the MAC address) of the STA.

Step 2: An AP returns the authentication result. The AP sends an authentication response that contains information indicating whether the authentication succeeds or fails. If the authentication succeeds, the STA and AP pass the bidirectional authentication.

Figure 1-5

↘ Shared-key Link Authentication

Shared-key link authentication is another authentication mechanism in addition to the open-system link authentication. Shared-key link authentication requires that the same shared key be configured for an STA and an AP. The shared-key link authentication can be configured only in static WEP encryption whereas the open-system link authentication is available in all the other modes.

The process of shared-key link authentication is as follows:

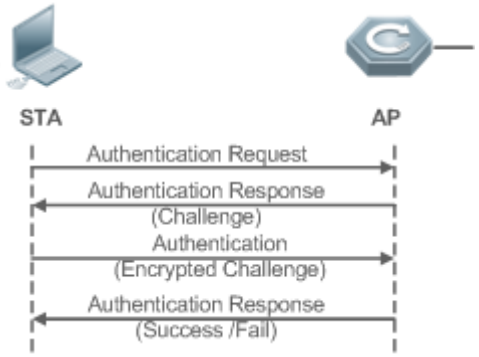
Step 1: An STA sends an authentication request to an AP.

Step 2: The AP generates a Challenge packet (a string) at random and sends the packet to the STA.

Step 3: The STA copies the received string to a new message, encrypts the message with a key and then sends the encrypted message to the AP.

Step 4: After receiving the message, the AP decrypts the message with the key, and then compares the decrypted string with the string sent to the STA. If the two strings are the same, it indicates that the STA has the same shared key as that on the AP and the shared-key authentication succeeds; otherwise, the shared-key authentication fails.

Figure 1-6



1.3.2 Access Authentication

Access authentication is a solution that enhances WLAN security.

After an STA is associated with an AP, whether the STA can use the service provided by the AP depends on the result of access authentication. If the STA passes the authentication, the AP enables the logical port for the STA; otherwise, the STA is not allowed to access the WLAN.

The IEEE 802.11 standard defines two access authentication approaches:

- PSK access authentication
- 802.1X access authentication

Working Principle

PSK Access Authentication

Pre-shared Key (PSK) is an 802.11i authentication mode, which performs authentication with pre-defined static keys. This authentication approach requires that an STA and an AP be configured with the same pre-shared key. If their keys are the same, the PSK access authentication succeeds; otherwise, the PSK access authentication fails.

802.1X Access Authentication

802.1X is a port-based network access control protocol. This authentication approach is used to authenticate and control the STAs at the port level. STAs connected to the ports can access resources in a WLAN if they pass the authentication; otherwise, the STAs cannot access resources in the WLAN.

A WLAN system with the 802.1X authentication function must provide the following elements to implement port-based authentication and authorization:

- Authentication client

Authentication client is generally installed on the STA. When the user wants to access the network, he activates the client program and enters the user name and password. Then, the client program sends a connection request.

- Authenticator

An authenticator means an AP or a communication device functioning as an AP. It is responsible for uploading and pushing user authentication information and enables or disables a port based on the authentication result.

- Authentication server

The authentication server checks whether a user has the right to use the services provided by the network system based on his identification information (user name and password), and enables or disables a port to the authentication system based on the authentication result.

MAB authentication uses a MAC address as the username to initiate a request to the authentication server. Therefore, it is not necessary for the terminal to install the client.

1.3.3 Wireless Data Encryption

Compared with a wired network, a wireless network is prone to greater security risks. Within an area, all WLAN devices share the same transmission medium and any device can receive data from all the other devices. This feature poses threat to WLAN data.

The IEEE 802.11i protocol defines the following encryption algorithms:

- WEP encryption
- TKIP encryption
- AES encryption

Working Principle

WEP Encryption

Wired Equivalent Privacy (WEP) is a data encryption mode specified in the original IEEE 802.11 standard, and is the basis for WLAN security authentication and encryption. WEP is used to promote the privacy of data exchanged between authorized users in a WLAN and prevent the data from being stolen.

WEP uses the RC4 algorithm to promote data privacy and implements authentication by using a shared key. WEP does not specify a key management scheme. Generally, keys are configured and maintained manually. WEP that does not provide a key distribution mechanism is called manual WEP or static WEP.

A WEP encrypted key may contain 64 bits or 128 bits. The 24-bit Initialization Vector (IV) is generated by the system. Therefore, a shared key to be configured on an AP and an STA consists of only 40 bits or 104 bits. In practice, the 104-bit WEP keys are widely used to replace the 40-bit WEP keys. WEP using 104-bit keys are called WEP-104. Although WEP-104 increases the security of WEP encryption, WEP encryption is prone to security risks due to limitations of the RC encryption algorithm and statically configured keys. WEP encryption cannot ensure the confidentiality and integrity of data or access authentication.

↘ TKIP Encryption

Temporal Key Integrity Protocol (TKIP) is a temporary makeshift solution created by the IEEE 802.11 organization for fixing the WEP encryption mechanism. Like WEP encryption, TKIP encryption also uses the RC4 algorithm. But compared with WEP encryption, TKIP encryption can provide much safer protection for WLAN services in the following aspects:

A static WEP key is manually configured and all users within the same service area share the same key. A TKIP key is generated through dynamic negotiation, and each packet has a unique key.

– TKIP increases the key length from 40 bits to 128 bits, and the IV length from 24 bits to 48 bits, thus improving the security of WEP encryption.

– TKIP supports Message Integrity Check (MIC) and the replay prevention function.

↘ AES Encryption

The Counter mode with CBC-MAC Protocol (AES-CCMP) is the most advanced wireless security protocol oriented to the public.

The IEEE 802.11i standard requires that CCMP be used to provide four security services, namely, authentication, confidentiality, integrity, and replay prevention. CCMP uses the 128-bit Advanced Encryption Standard (AES) to implement confidentiality and uses the CBC-MAC to ensure data integrity and authentication.

As a new advanced encryption standard, AES uses the symmetrical block encryption technology to provide better encryption performance than the RC4 algorithm in WEP/TKIP. It is the new-generation encryption technology that replaces WEP and brings more powerful security protection for WLANs.

The IEEE 802.11r standard requires that CCMP be used to encrypt EAPOL packets. Therefore, before enabling the 802.11r function, configure the AES-CCMP encryption mode.

1.3.4 WPA3 Authentication

Compared with WPA2 PSK mode, the WPA3 Personal mode have the new SAE interaction, which is borne over authentication packets. When an AP/AC interacts with an STA, there are only one pair of authentication packets (two packets) in WPA2 PSK mode and two pairs of authentication packets (four packets) in WPA3 Personal mode. In the SAE process, parameters interacted using public and private keys and various random numbers are carried in SAE packets and a PMK is negotiated using passwords of the AP/AC and the STA. The PMK is then used for 4-way handshake. In WPA2 mode, PMKs used for 4-way handshake map to passwords and therefore PMKs can be cracked via dictionary attacks. 256-bit random numbers are added to the SAE interaction and cracking is impossible. Therefore, the restriction that the password length cannot be shorter than 8 characters is eliminated in WPA3 Personal mode.

In WPA3 Enterprise mode, the overall security is improved from 128-bit encryption to 192-bit encryption. The unicast key length increases from 128 bits to 256 bits, the multicast encryption suite is changed from CCMP to GCMP-256, and the multicast management suite is changed from CCMP to BIP-GMAC-256.

1.4 Configuration

Configuration	Description and Command	
Configuring Static WEP	(Mandatory) It is used to enable static WEP encryption.	
	security static-wep-key encryption	Enables static WEP for a WLAN and configures a static WEP key.
	(Optional) It is used to configure the link authentication mode.	
	security static-wep-key authentication	Configures the link authentication mode of static WEP.
Configuring WPA Authentication	(Mandatory) It is used to enable WPA authentication.	
	security wpa	Configures WPA authentication.
	security wpa ciphers	Configures the encryption mode of WPA authentication.
	security wpa akm	Configures the access authentication mode for WPA authentication.

Configuration	Description and Command	
	(Optional) It is used to configure a shared key for WPA PSK authentication.	
	security wpa akm psk set-key	Configures a shared key for WPA PSK authentication.
Configuring RSN Authentication	(Mandatory) It is used to enable RSN authentication.	
	security rsn	Configures RSN authentication.
	security rsn ciphers	Configures the encryption mode for RSN authentication.
	security rsn akm	Configures the access authentication mode for RSN authentication.
	(Optional) It is used to configure a shared key for RSN PSK authentication.	
	security rsn akm psk set-key	Configures a shared key for RSN PSK authentication.
Configuring MAB Authentication	(Optional) It is used to configure MAB authentication.	
	dot1x-mab	Enables MAB authentication.
Configuring Authentication Parameters	(Optional) It is used to configure key interaction parameters and the jitter prevention time in WEB authentication.	
	authtimeout forbidcount	Configures the association forbidding count after four-way handshake key interaction fails.
	authtimeout forbidtime	Configures the association forbidding interval after four-way handshake key interaction fails.
	authtimeout groupcount	Configures the multicast key negotiation packet re-transmission count.
	authtimeout grouptime	Configures the timeout duration of multicast key negotiation packets.
	authtimeout paircount	Configures the uncast key negotiation packet re-transmission count.
	authtimeout pairtime	Configures the timeout duration of unicast key negotiation packets.
	webauth prevent-jitter	Configures the jitter prevention time of WEB authentication.
Configuring WPA3	**security wpa3 dot11r**	Enables or disables the WPA3 802.11r function.
	security wpa3 mode	Sets the WPA3 mode.
	security wpa3 personal passphrase	Sets a password for the WPA3 Personal mode.

1.4.1 Configuring Static WEP

Configuration Effect

- Enable static WEP encryption and provide WEP encryption protection for WLAN data.
- Configure the link authentication mode.

Notes

- The link authentication mode must be configured after static WEP encryption is enabled.
- In the security mode of a WLAN, static WEP encryption cannot be configured together with other authentication encryption.
- Only one WLAN can be configured with static WEP encryption

Configuration Steps

↘ Enabling Static WEP

- Mandatory.
- Enable static WEP encryption in WLAN security configuration mode on the AC.

Command	**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*
Parameter Description	*key-length*: Specifies the key length, which can be 40 bits or 104 bits. **ascii**: Specifies that the WEP key is ASCII code. **hex**: Specifies that the WEP key is hexadecimal code. *key-index*: Specifies the key index, ranging from 1 to 4. *key*: Specifies key data.
Defaults	Static WEP is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure a static WEP key and enable static WEP. This command can be configured repeatedly, but only the last configuration takes effect. The key length must be the same as the *key-length* parameter in the command.

↘ Configuring the Link Authentication Mode

- (Optional) The default link authentication mode is open-system link authentication. This command can be used to configure shared-key link authentication.
- Enable static WEP encryption in security configuration mode on the AC.
- The link authentication mode can be configured only after static WEP encryption is enabled. After configuring the sharedkey link authentication mode, set the link authentication mode to shared key link authentication on the STA; otherwise, the STA cannot access the WLAN.

Command	**security static-wep-key authentication** { **open** | **share-key** }
Parameter	**open**: Configures open-system link authentication.

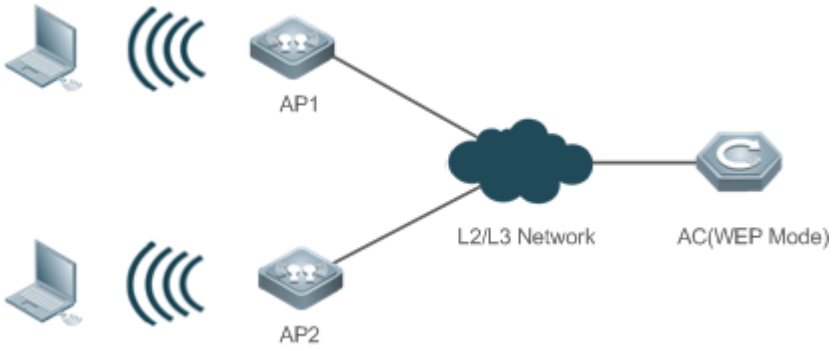
Description	**share-key**: Configures shared key link authentication.
Defaults	An STA accesses a WLAN by using open-system link authentication by default.
Command Mode	WLAN security configuration mode
Usage Guide	Configure the link authentication mode after configuring a static WEP key. The link authentication mode cannot be configured for other security configuration modes than static WEP.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring Static WEP Encryption and Using Shared-Key Link Authentication for WLAN 1

Scenario Figure 1-7	 In a Fit AP environment, configure WLAN 1 on the AC and configure the security policies 1 as follows: 1. Enable static WEP encryption. 2. Configure shared-key link authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable static WEP encryption and configure a WEP key. ● Set the link authentication mode to shared-key link authentication.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345` `Ruijie(config-wlansec)#security static-wep-key authentication share-key`
Verification	Run the **show running-config	begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config	begin wlansec 1` `wlansec 1` ` security static-wep-key encryption 40 ascii 1 12345`

	security static-wep-key authentication share-key !

Common Errors

- The configured key length is inconsistent with the specified key length.
- Static WEP is configured for multiple WLANs.
- The link authentication mode is configured before static WEP is enabled.

1.4.2 Configuring WPA Authentication

Configuration Effect

- Enable WPA authentication for a WLAN.
- Specify the access authentication mode and encryption mode in WPA authentication.

Notes

- When WPA authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, WPA authentication cannot be configured with WEP authentication.

Configuration Steps

↘ Configuring WPA Authentication

- Mandatory.
- Enable WPA authentication in WLAN security configuration mode on the AC.

Command	**security wpa** { **enable** | **disable** }
Parameter Description	**enable**: Enables WPA authentication. **disable**: Disables WPA authentication.
Defaults	WPA authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in WPA authentication only after WPA authentication is enabled; otherwise, the configuration does not take effect. When WPA authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

↘ Configuring the Encryption Mode of WPA Authentication

- Mandatory.

- It is configured in WLAN security configuration mode on the AC.
- The encryption mode of WPA authentication can be configured only after WPA authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between an STA and the WLAN is protected by the corresponding encryption mode.

Command	**security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode of WPA authentication. **disable**: Disables the encryption mode of WPA authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode of WPA authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode of WPA authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security wpa akm** { **psk** | **802.1x** } { **enable** | **disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode of WPA authentication. **disable**: Disables the access authentication mode of WPA authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after WPA authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for WPA Authentication

- (Optional) It must be configured when WPA PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

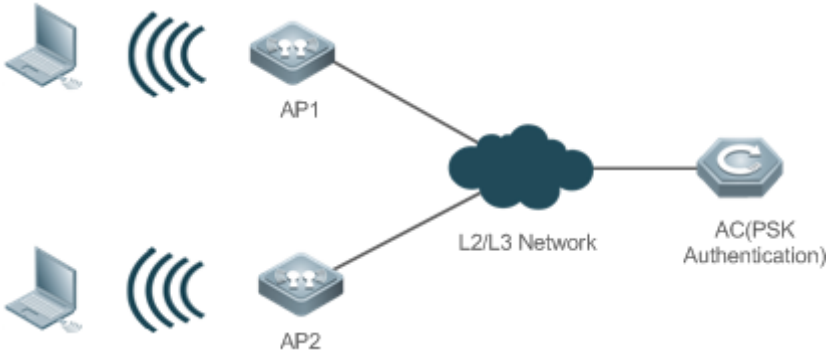
Command	**security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring WPA PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario Figure 1-8	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure WPA PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable WPA authentication. ● Configure the AES encryption mode for WPA authentication. ● Configure the PSK access authentication mode for WPA authentication. ● Configure the PSK key 12345678.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security wpa enable` `Ruijie(config-wlansec)#security wpa ciphers aes enable`

	Ruijie(config-wlansec)#security wpa akm psk enable Ruijie(config-wlansec)#security wpa akm psk set-key ascii 12345678
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	Ruijie#show running-config | begin wlansec 1 wlansec 1 security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 12345678 !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- A WPA encryption mode is configured before WPA authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before WPA authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- A WPA PSK key is configured before WPA authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.3 Configuring RSN Authentication

Configuration Effect

- Enable RSN authentication for a WLAN.
- Specify the access authentication mode and encryption mode in RSN authentication.

Notes

- When RSN authentication is used, the encryption mode and access authentication mode must also be configured.
- If the access authentication mode is set to PSK, a PSK key must be configured.
- In the security mode of a WLAN, RSN authentication cannot be configured with WEP authentication.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured in RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The encryption mode in RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After an encryption mode is configured for a WLAN, communication data between an STA and the WLAN is protected by the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode for RSN authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.

- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode in RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN that is enabled with access authentication only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

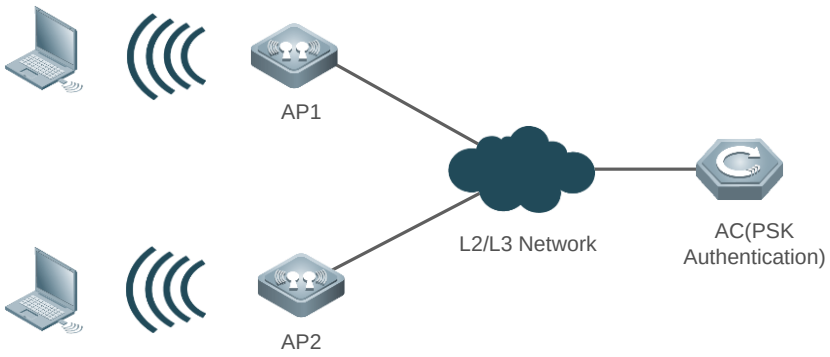
Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	This shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring RSN PSK Authentication, AES Encryption and Key 12345678 for WLAN 1

Scenario **Figure 1-9**	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure RSN PSK authentication. 2. Configure the AES encryption mode. 3. Configure the shared key to 12345678.
Configuration Steps	● Access security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security rsn enable` `Ruijie(config-wlansec)#security rsn ciphers aes enable` `Ruijie(config-wlansec)#security rsn akm psk enable` `Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678`
Verification	Run the **show running-config	begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config	begin wlansec 1` `wlansec 1` ` security rsn enable` ` security rsn ciphers aes enable` ` security rsn akm psk enable` ` security rsn akm psk set-key ascii 12345678` `!`

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- An RSN encryption mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- An access authentication mode is configured before RSN authentication is enabled in WLAN security configuration mode.
- If an access authentication mode is enabled in WLAN security configuration mode, no other access authentication mode can be configured.
- An RSN PSK key is configured before RSN authentication is enabled.
- The ASCII key consists of less than 8 characters or more than 63 characters.
- The hexadecimal key does not consist of 64 characters.

1.4.4 Configuring RSN 802.11r

Configuration Effect

- If the 802.11r function is enabled for a WLAN, the 802.1x authentication and 4-way handshake are not required during fast roaming, thereby reducing network delay caused by roaming.

Notes

- 802.11r can be independently configured in RSN and WPA3.
- The RSN 802.11r function can be enabled only when the following conditions are met:
    1. RSN authentication is enabled.
    2. WPA authentication is disabled, that is, WPA and RSN cannot be enabled simultaneously.
    3. The access authentication mode (AKM) is configured as PSK or 802.1x.
    4. AES encryption is enabled.
    5. TKIP encryption is disabled, that is, AES and TKIP cannot be enabled simultaneously.
- For roaming between ACs with the same SSID, WLAN IDs of the ACs must be the same.
- The 802.1x LEAP authentication mode is not supported.

Configuration Steps

↘ Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.

Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured for RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The encryption mode for RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After a data encryption mode is configured for a WLAN and a STA accesses the WLAN, communication data of the STA is protected in the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable the AES or TKIP encryption mode for RSN authentication. To use the 802.11r function, AES encryption must be configured. In addition, TKIP encryption must be disabled. TKIP encryption is disabled by default.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode for RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN with access authentication enabled only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication.

	disable: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is an ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 characters. **hex**: Specifies that the PSK key is a hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	The shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Enabling RSN 802.11r

- Optional

Command	**security rsn dot11r {disable | enable}**
Parameter Description	**disable**: Disables 802.11r. **enable**: Enables 802.11r.
Defaults	The 802.11r function is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	To manually enable the 802.11r function, a judgment is made based on the conditions. For details about the conditions, see "Notes." This command is valid only when AKM (802.1x or PSK) is enabled. This command is valid only when AES encryption is enabled.

Modifying 802.11r Re-association Timeout Duration

- (Optional) This command is used to configure the re-association timeout duration in the unit of seconds (that is, the maximum interval for a client to send an association request after the client authentication is completed).

Command	**security rsn dot11r reassoc-timeout** *timeout*

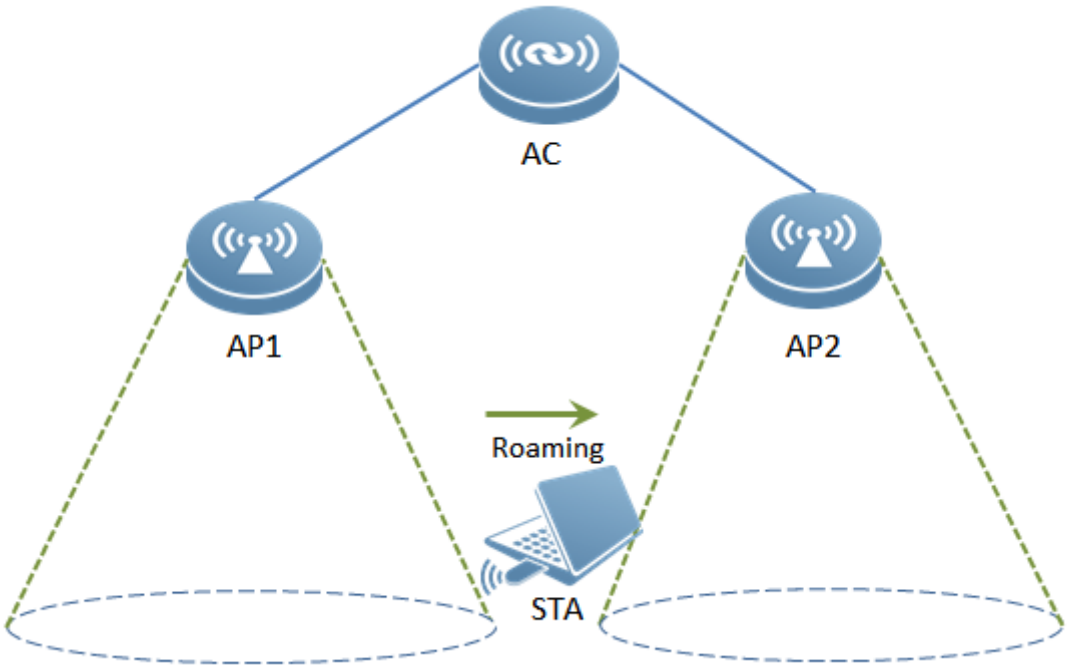
Parameter Description	*timeout:* The range is from 1 to 120. The unit is second.
Defaults	The re-association timeout duration is 20 seconds by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command takes effect only after the 802.11r function is enabled. If the client does not initiate an re-association request within the re-association timeout duration, the roaming is stopped.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

↘ Configuring RSN PSK Authentication, AES Encryption, and Key 12345678 and Enabling 802.11r for WLAN 1

Scenario **Figure 1-10**	 In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure RSN PSK authentication. 2. Configure AES data encryption. 3. Set the shared key to 12345678. 4. Enable 802.11r.
Configuration	● Enter the security configuration mode of WLAN 1.

Steps	● Enable RSN authentication. ● Set the data encryption mode for RSN authentication to AES. ● Set the access authentication mode for RSN authentication to PSK. ● Set the PSK key to 12345678. ● Enable 802.11r.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security rsn enable` `Ruijie(config-wlansec)#security rsn ciphers aes enable` `Ruijie(config-wlansec)#security rsn akm psk enable` `Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678` `Ruijie(config-wlansec)#security rsn dot11r enable`
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config | begin wlansec 1` `wlansec 1` ` security rsn enable` ` security rsn ciphers aes enable` ` security rsn akm psk enable` ` security rsn akm psk set-key ascii 12345678` ` security rsn dot11r enable` `!`

Common Errors

- 802.11r is enabled while RSN authentication is disabled or both of RSN and WPA are enabled .
- 802.11r is enabled while the authentication mode (802.1x or PSK) is not configured.
- 802.11r is enabled while AES encryption is disabled or both of AES encryption and TKIP encryption are enabled.
- The SSIDs of ACs are the same but the WLAN IDs are different, causing FT roaming failures.

1.4.5 Configuring WPA3 802.11r

Configuration Effect

- If the 802.11r function is enabled for a WLAN, the 802.1x authentication and 4-way handshake are not required during fast roaming, thereby reducing network latency caused by roaming handover.

Notes

- 802.11r can be independently configured in RSN and WPA3.

Configuration Steps

Enabling WPA3 802.11r

- Mandatory.
- Set the WPA3 mode to **Personal** or **Enterprise** before enabling the 802.11r function.

Command	**security wpa3 dot11r** { **enable** | **disable** }
Parameter Description	**enable**: Enables the 802.11r function in WPA3 mode. **disable**: Disables the 802.11r function in WPA3 mode.
Defaults	The 802.11r function is disabled in WPA3 mode by default.
Command Mode	WLAN security configuration mode
Usage Guide	Set the WPA3 mode to **Personal** or **Enterprise** before using the 802.11r fast roaming function in WPA3 mode.

1.4.6 Configuring MAB Authentication

Configuration Effect

- Enable MAB authentication for a WLAN.

Notes

- In security mode of a WLAN, MAB authentication cannot be configured together with 802.1X access authentication or WEP authentication, but can be configured together with PSK authentication.

Configuration Steps

Configuring MAB Authentication

- Mandatory.
- Enable MAB authentication in WLAN security configuration mode on the AC.
- Run the **dot1x-mab** command to enable MAB authentication or run the **no dot1x-mab** command to disable MAB authentication.
- MAB authentication can be configured independently, without RSN or WPA authentication enabled. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

Command	**dot1x-mab**

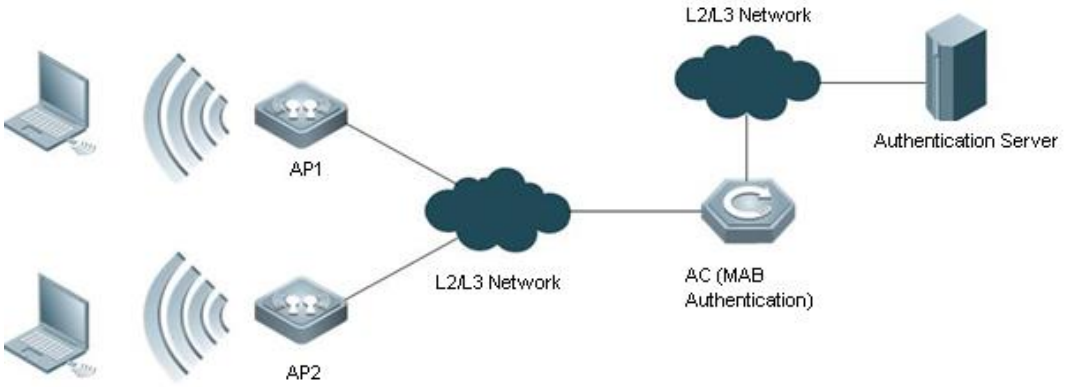
Parameter Description	**no**: Disables MAB authentication.
Defaults	MAB authentication is not configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable MAB authentication. MAB authentication can be used together with PSK access authentication, but cannot be used together with 802.1X access authentication.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring MAB Authentication for WLAN 1

Scenario Figure 1-11	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure MAB authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable MAB authentication.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#dot1x-mab`
Verification	Run the **show running-config	begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config	begin wlansec 1` `wlansec 1` ` dot1x-mab` `!`

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP).
- If 802.1X access authentication is enabled in WLAN security configuration mode, MAB authentication cannot be configured.

1.4.7 Configuring Authentication Parameters

Configuration Effect

- Configure key interaction parameters.
- Configure the jitter prevention time in WEB authentication.

Notes

- Key interaction parameters take effect only in PSK or 802.1X authentication.
- The jitter prevention time in WEB authentication can be configured only after WEB authentication is enabled.

Configuration Steps

↘ Configuring Key Interaction Parameters

- Optional. Generally, it is unnecessary to configure key interaction parameters. It is recommended to set the packet re-transmission count and timeout duration to great values for a poor WLAN environment.
- It is configured in WLAN security configuration mode on the AC.

Command	**authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }
Parameter Description	**forbidcount** *count*: Configures the association forbidding count after four-way handshake key interaction fails.. **forbidtime** *time*: Configures the association forbidding interval after four-way handshake key interaction fails. **groupcount** *count*: Configures the multicast key negotiation packet re-transmission count. **grouptime** *timeout*: Configures the timeout duration of multicast key negotiation packets. **paircount** *count*: Configures the unicast key negotiation packet re-transmission count. **pairtime** *timeout*: Configures the timeout duration of unicast key negotiation packets.
Defaults	The association is not forbidden after four-way handshake key interaction fails. The default multicast key negotiation packet re-transmission count is 4. The default timeout duration of multicast key negotiation packets is 1200 ms. The default unicast key negotiation packet re-transmission count is 4. The default timeout duration of unicast key negotiation packets is 1200 ms.
Command Mode	WLAN security configuration mode
Usage Guide	Key interaction parameters take effect only in PSK or 802.1X authentication.

Configuring the Jitter Prevention Time of WEB Authentication

- Optional. The default jitter prevention time of WEB authentication is 300 seconds. Users can configure the jitter prevention time based on actual requirements or disable the jitter prevention of WEB authentication by setting the time to 0 seconds.
- It is configured in WLAN security configuration mode on the AC.

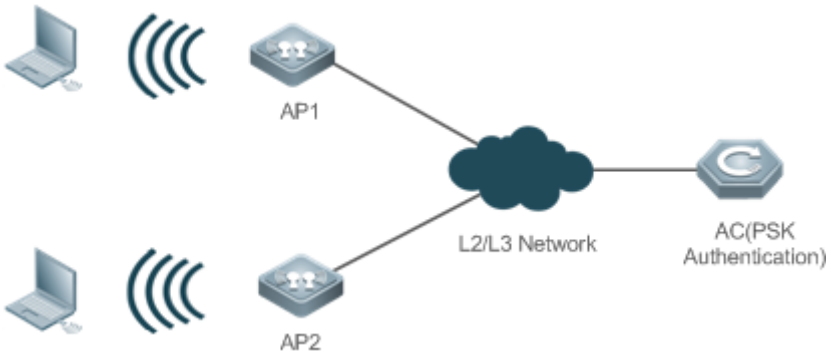
Command	**webauth prevent-jitter** *timeout*
Parameter Description	*timeout*: Configures the jitter prevention time of WEB authentication, ranging from 0 to 86400 seconds (the jitter prevention of WEB authentication is disabled when this parameter is set to 0).
Defaults	The default jitter prevention time of WEB authentication is 300 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	The jitter prevention time of WEB authentication can be configured only after WEB authentication is enabled.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring the RSN-PSK + WEB Authentication Mode, the Unicast Key Negotiation Re-transmission Count to 5, and the Jitter Prevention Time of WEB Authentication to 900 Seconds for WLAN 1

Scenario Figure 1-12	 In a Fit AP environment, configure the security policies of WLAN 1 on the AC as follows: 1. Configure RSN PSK authentication. 2. Enable WEB authentication.
Configuration Steps	● Access the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Configure the AES encryption mode for RSN authentication. ● Configure the PSK access authentication mode for RSN authentication. ● Configure the PSK key 12345678. ● Set the unicast key negotiation packet re-transmission count to 5.

	• Configure WEB authentication. • Set the jitter prevention time of WEB authentication to 900 seconds.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security rsn enable` `Ruijie(config-wlansec)#security rsn ciphers aes enable` `Ruijie(config-wlansec)#security rsn akm psk enable` `Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678` `Ruijie(config-wlansec)#authtimeout paircount 5` `Ruijie(config-wlansec)#webauth` `Ruijie(config-wlansec)#webauth prevent-jitter 900`
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config | begin wlansec 1` `wlansec 1` ` security rsn enable` ` security rsn ciphers aes enable` ` security rsn akm psk enable` ` security rsn akm psk set-key ascii 12345678` ` webauth prevent-jitter 900` ` webauth` ` authtimeout paircount 5`

Common Errors

- The jitter prevention time of WEB authentication is configured before WEB authentication is enabled.

1.4.8 Configuring Management Frame Encryption

Configuration Effect

- Transmit partial management frames over the air interface in ciphertext format.

Notes

- Only WPA2 supports management frame encryption. If the WLAN uses Open, WEP-40, WEP-104 or WPA (AES or TKIP) for encryption, the management frame encryption function cannot be enabled.
- Not all STAs' OSs support management frame encryption.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured for RSN authentication only after RSN authentication is enabled; otherwise, the configuration does not take effect. When RSN authentication is used, the encryption mode and access authentication mode must also be configured. If either the encryption mode or the access authentication mode is configured or neither of them is configured, STAs cannot access a WLAN.

Configuring the Encryption Mode for RSN Authentication

- Mandatory.
- It is configured in WLAN security configuration mode on the AC.
- The encryption mode for RSN authentication can be configured only after RSN authentication is enabled. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode. After a data encryption mode is configured for a WLAN and a STA accesses the WLAN, communication data of the STA is protected in the corresponding encryption mode.

Command	**security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }
Parameter Description	**aes**: Configures the AES encryption mode. **tkip**: Configures the TKIP encryption mode. **enable**: Enables the encryption mode for RSN authentication. **disable**: Disables the encryption mode for RSN authentication.
Defaults	No encryption mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable the AES or TKIP encryption mode for RSN authentication. The AES and TKIP encryption modes can be enabled at the same time in WLAN security configuration mode.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.

- It is configured in WLAN security configuration mode on the AC.
- The access authentication mode for RSN authentication can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode. An STA can access a WLAN with access authentication enabled only after passing the access authentication.

Command	**security rsn akm** { **psk** | **802.1x** } { **enable | disable** }
Parameter Description	**psk**: Sets the access authentication mode to pre-shared key authentication. **802.1x**: Sets the access authentication mode to 802.1X authentication. **enable**: Enables the access authentication mode for RSN authentication. **disable**: Disables the access authentication mode for RSN authentication.
Defaults	No access authentication mode is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only after RSN authentication is enabled. Only one access authentication mode can be enabled for a WLAN in security configuration mode.

Configuring a Shared Key for RSN Authentication

- (Optional) It must be configured when RSN PSK authentication is enabled.
- It is configured in WLAN security configuration mode on the AC.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is an ASCII code. *ascii-key*: Specifies a key in the ASCII format, consisting of 8 to 63 characters. **hex**: Specifies that the PSK key is a hexadecimal code. *hex-key*: Specifies a key in the hexadecimal format, consisting of 64 characters.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	The shared key takes effect only when PSK authentication is enabled. A key in the ASCII format consists of 8 to 63 characters. A key in the hexadecimal format consists of 64 characters.

Enabling Management Frame Encryption

- Mandatory.
- Enable management frame encryption on an AC.
- Management frame encryption can be configured only after RSN authentication is enabled.

Command	**security pmf** { **mandatory** | **optional | disable** }
Parameter Description	**mandatory**: The client needs to support management frame encryption. **optional**: The client does not need to support management frame encryption. **Disable**: Disables management frame encryption.

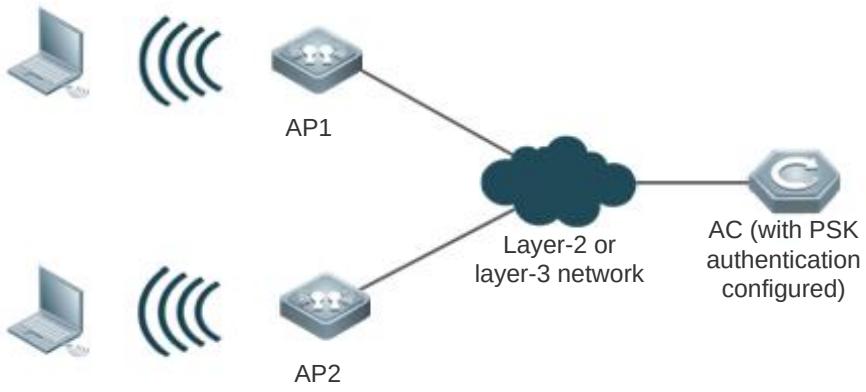
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Enabling RSN-PSK Authentication and Management Frame Encryption for WLAN 1

Scenario Figure 1-13	 In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure RSN PSK authentication. 2. Enable management frame encryption.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable RSN authentication. ● Set the data encryption mode for RSN authentication to AES. ● Set the access authentication mode for RSN authentication to PSK. ● Set the PSK key to 12345678. ● Enable management frame encryption.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security rsn enable` `Ruijie(config-wlansec)#security rsn ciphers aes enable` `Ruijie(config-wlansec)#security rsn akm psk enable` `Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678` `Ruijie(config-wlansec)#security rsn pmf mandatory`

Verification	Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config | begin wlansec 1` `wlansec 1` ` security rsn enable` ` security rsn ciphers aes enable` ` security rsn akm psk enable` ` security rsn akm psk set-key ascii 12345678` ` security rsn pmf mandatory`

Common Errors

- WPA encryption is configured, but management frame encryption cannot be enabled.
- After **mandatory** is specified, an STA cannot go online because the STA does not support management frame encryption.

1.4.9 Configuring WPA3 Authentication

Configuration Effect

- Enable the WPA3 authentication mode on a WLAN.

Notes

- WPA3 is incompatible with WPA. After either of them is enabled, related prompts are displayed on the CLI if you attempt to enable the other one.
- WPA3 is incompatible with WPA2+TKIP. After either of them is enabled, related prompts are displayed on the CLI if you attempt to enable the other one.
- The WPA3 Enterprise mode is incompatible with WPA2. After either of them is enabled, related prompts are displayed on the CLI if you attempt to enable the other one.
- WPA3 relies on management frame encryption, which needs to be enabled first. Related prompts will be displayed on the CLI.

Configuration Steps

↘ Configuring Management Frame Encryption

- Mandatory.
- Perform the configuration in security configuration mode on a WLAN on the AC.

Command	**security pmf** {**optional** | **mandatory** | **disable** }

Parameter Description	**mandatory**: Indicates that the client needs to support management frame encryption. **optional**: Indicates that management frame encryption is optional on the client. **disable**: Disables management frame encryption.
Defaults	Management frame encryption is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuring the WPA3 Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 mode to **Personal**, **Enterprise**, or **Enhanced-Open**.

Command	**security wpa3 mode** { **none | personal** | **enterprise| enhanced-open**}
Parameter Description	**none**: Indicates that WPA3 is disabled. **personal**: Indicates the WPA3 Personal mode, in which shared passwords are used for authentication. **enterprise**: Indicates the WPA3 Enterprise mode, in which 802.1x is used for authentication. **enhanced-open**: Indicates the WPA3 Enhanced-Open mode, in which 802.1x is used for authentication.
Defaults	WPA3 is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	WPA3 is incompatible with WPA, the WPA3 Personal mode is compatible with WPA2, the WPA3 Enterprise mode is incompatible with WPA2, and the WPA3 Enhanced-Open mode is incompatible with WPA and WPA2.

Configuring a Password for the WPA3 Personal Mode

- The configuration is optional if WPA2 PSK authentication is enabled but mandatory when only the WPA3 Personal mode is enabled.
- Configure a password for the WPA3 Personal mode. If no password is configured, WPA2 PSKs are used.

Command	**security wpa3 personal passphrase** { **none** | *p* }
Parameter Description	**none**: Clears the password. *p*: Indicates a password in ASCII code, consisting of 1 to 63 characters.
Defaults	No password is configured for the WPA3 Personal mode by default.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

↘ Configuring the WPA3 Personal Authentication Mode for WLAN 1 and Setting the Password to 1

Scenario	In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure the pure WPA3 Personal authentication mode (RSNA disabled). 2. Set the shared key to 1.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable management frame encryption. ● Set the password to 1 for the WPA3 Personal mode. ● Set the WPA3 mode to Personal.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security pmf optional` `Ruijie(config-wlansec)#security wpa3 personal passphrase 1` `Ruijie(config-wlansec)#security wpa3 mode personal`
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config | begin wlansec 1` `wlansec 1` ` security pmf optional` ` security wpa3 personal passphrase 1` ` security wpa3 mode personal`

Common Errors

- If you attempt to enable WPA authentication on a WLAN in WPA3 Personal or Enterprise mode, a configuration failure will be displayed.
- If you attempt to enable WPA2 (RSNA) authentication and set the cipher to TKIP in WPA3 Personal mode, a configuration failure will be displayed.
- If you attempt to enable WPA2 (RSNA) authentication on a WLAN in WPA3 Enterprise mode, a configuration failure will be displayed.

1.5 Monitoring

Displaying

Description	Command
Displays security configuration of a WLAN.	**show wlan security** *wlan-id*
Displays security configuration of an STA.	**show wclient security** *mac-address*

2 Configuring WIDS

2.1 Overview

Compared with wired networks, Wireless LAN (WLAN) has unparalleled advantages, such as convenient deployment, flexible use, efficient cost, and easy extension, making it more and more prevalent. However, for the openness of its channels, WLAN is much vulnerable to various network threats, such as rogue access points (APs), Ad-hoc networks, and all types of protocol attacks. Therefore, security becomes a major factor that hinders WLAN development.

Wireless Intrusion Detection System (WIDS) detects vicious STA attacks and invasions in the early stage, which helps network administrators actively observe and defend against the hidden dangers in networks in the first time.

2.2 Applications

Application	Description
Frame Filtering	Facing illegal STAs attempting to access WLAN, WIDS frame filtering helps control STA access.
User Isolation	Facing an STA intending to visit other STAs in WLAN, WIDS user isolation helps isolate their direct communication.
IDS	Facing all kinds of invasion attacks in WLAN, Intrusion Detection System (IDS) helps detect those attacks.
Rogue Detection and Containment	Illegal or rogue devices in WLAN jeopardize STAs and normal services by faking services. Facing it, Rogue detection and containment help monitor and contain them.

2.2.1 Frame Filtering

Scenario

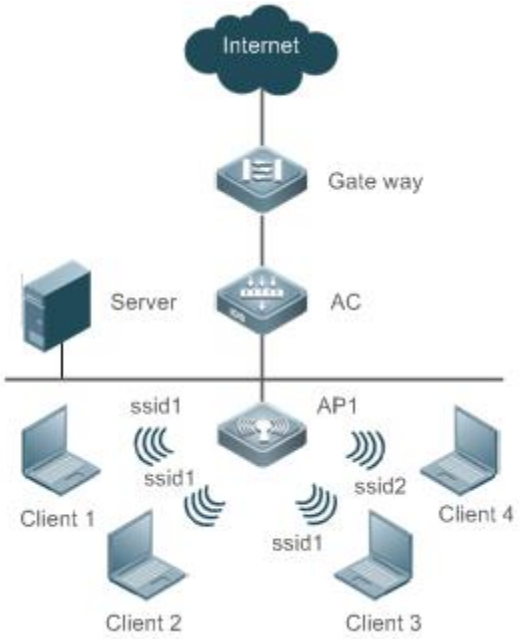
The wireless access control service is provided in WLAN, including allowing specified STAs to access WLAN or specified networks, forbidding STAs from accessing WLAN or specified networks, forbidding low-rate stations (STAs) from accessing WLAN, as well as dynamically controlling network access.

The figure below is an example, assuming that there are the following deployment requirements in the network:

- Allow Client 1 to access WLAN and Client 2 to access SSID 1.
- Prohibit Client 3 from accessing WLAN and Client 4 from accessing SSID 2.
- Filter and kick out low-rate STAs.
- Dynamically control STA access.

The networking topology is shown as follows:

Figure 2-1 Networking Topology of Wireless Access Control



Deployment

The key configuration points for the devices are:

- Add Client 1 to a WIDS whitelist. As a result, Client 1 can access the WLAN service provided by all APs under the AC. Other STAs not in the list cannot.
- Add Client 2 to the SSID 1-based whitelist. As a result, Client 2 can access SSID 1 provided by all APs under the AC. Other STAs not in the list cannot.
- Add Client 3 to a static blacklist. As a result, Client 3 cannot access the WLAN service provided by all APs under the AC.
- Add Client 4 to the SSID 1-based blacklist. As a result, Client 4 cannot access SSID 1 provided by all APs under the AC.
- Configure the low-rate threshold. STAs of an AC with rates less than the threshold will be kicked out.
- Enable the dynamic blacklist function, supporting the IDS function. After the dynamic blacklist function is enabled, any detected attack will be added into the dynamic blacklist. When the blacklist is within aging duration, the listed STAs will continue to be forbidden from communication accessed by the current AP.

2.2.2 User Isolation

Scenario

Layer-2 user isolation is provided in WLAN, including AP-based, AP-SSID based, AC-based, AC-SSID based, and SSID-based.

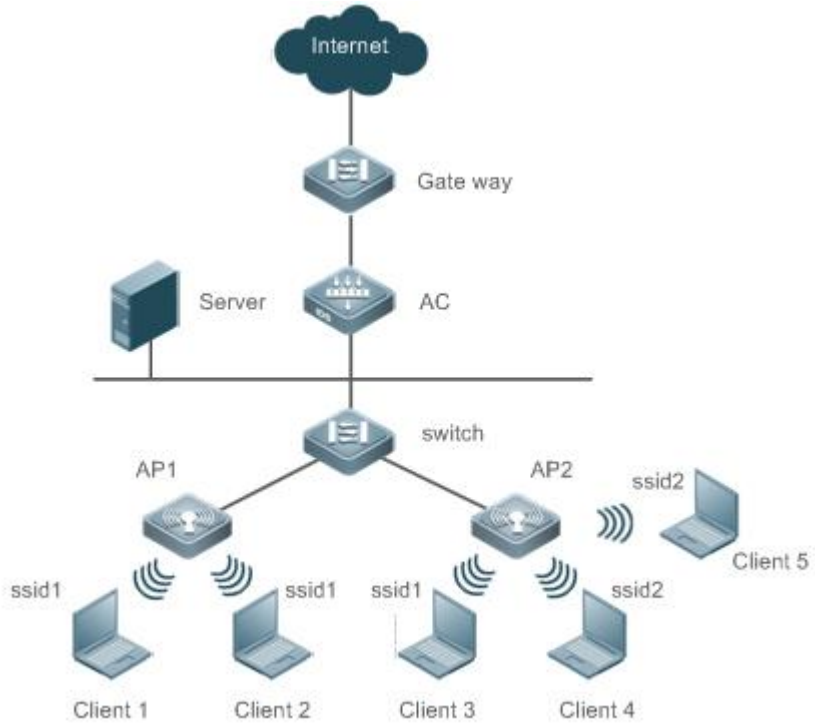
Assuming there are the following deployment requirements in the network:

Client 1 to Client 3 are associated with SSID 1, and Client 4 and Client 5 are associated with SSID 2. SSID 1 and SSID 2 are mapped to the same VLAN. Client 1 to Client 5 are layer-2 users.

- Direct communication cannot be conducted between Client 1 and Client 2, and among Client 3 to Client 5, but can be done among other users.
- Direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5, but can be done among other users.
- Direct communication cannot be conducted between Client 1 and Client 3, Client 4 or Client 5, and between Client 2 and Client 3, Client 4 or Client 5, but can be done among other users.
- Direct communication cannot be conducted between Client 3 and Client 1 or Client 2, but can be done among other users.
- Direct communication cannot be conducted among Client 1 to Client 3, but can be done among other users.

The networking topology is shown as follows:

Figure 2-2 Networking Topology of Wireless User Isolation



Deployment

The key configuration points for the devices are:

- Configure AP-based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 2, and among Client 3 to Client 5.
- Configure AP-SSID based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5.

- Configure AC-based user isolation. As a result, direct communication cannot be conducted between Client 1 or Client 2 and Client 3 to Client 5.
- Configure AC-SSID based user isolation. As a result, direct communication cannot be conducted between Client 3 and Client 1 or Client 2.
- Configure SSID 1-based user isolation. As a result, direct communication cannot be conducted among Client 1, Client 2 and Client 3.

2.2.3 IDS

Scenario

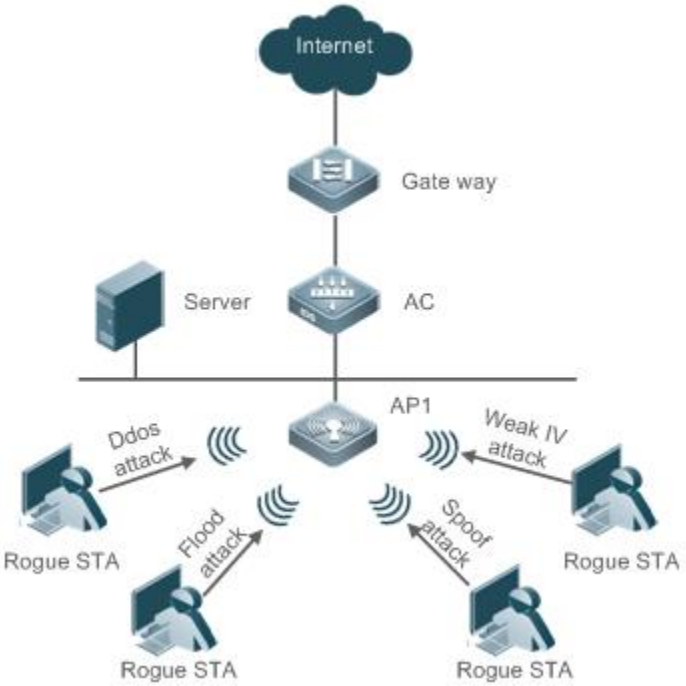
Wireless invasion attacks exist in networks, including Distributed Denial of Service (DDoS), spoofing, flooding, and Weak IV attacks. It requires APs to detect these attacks and carry out countermeasures.

Assuming there are the following deployment requirements in the network:

- DDoS attacks
- Spoofing attacks
- Flooding attacks
- Weak IV attacks

The networking topology is shown as follows:

Figure 2-3 Networking Topology of IDS



Deployment

The key configuration points for the devices are:

- Enable DDoS detection with thresholds specified which perform statistics of ARP, SYN and ICMP attack packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the spoofing detection with related thresholds specified to detect the deauthentication and disassociation packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable flooding detection with related thresholds specified to detect the Authentication, Association, Reassociation, Deauthentication, Disassociation, Probe, Null data and Action packets. If any threshold is exceeded, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.
- Enable the Weak IV detection with related thresholds specified to detect the IV value of the Web packets. If the number of continuous attacks exceeds the threshold, the detection results will be logged, and the users will be blacklisted if the dynamic blacklist is enabled.

2.2.4 Rogue Detection and Containment

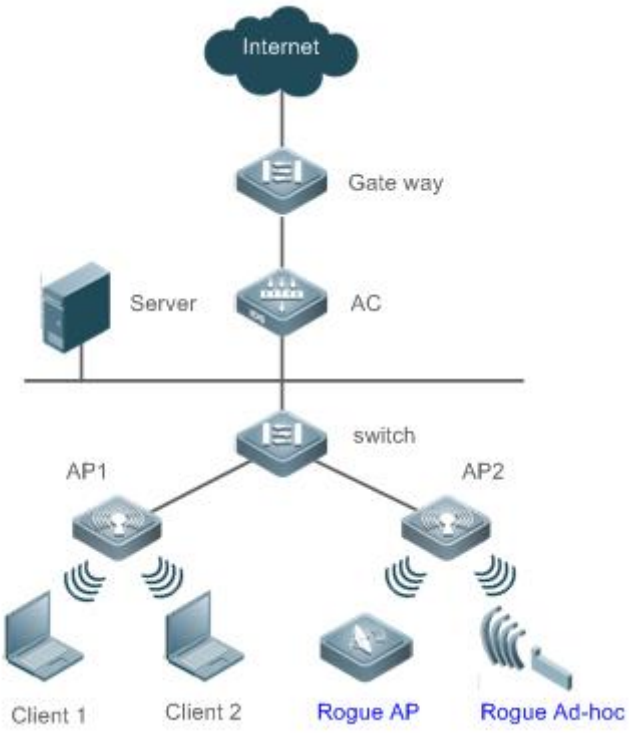
Scenario

Assuming there is the following deployment requirement in the network:

- Rogue AP and Ad-hoc devices exist in network, and detection and containment are required.

The networking topology is shown as follows:

Figure 2-4 Networking Topology of Rogue Detection and Containment



Deployment

The key configuration points for devices are:

- Enable the Monitor or Hybrid mode for a specified AP, and start the detection timer of the AP and obtain detected data at the end of each period.
- Enable the device containment and configure the mode.
- Counter the Rogue APs and Ad-hoc devices regularly based on the containment mode and detected data, preventing users from associating with fake services.

2.3 Features

Basic Concepts

Working Modes

The WIDS has the following working modes:

- Normal mode, providing only the access service
- Monitor mode, providing only the monitoring service
- Hybrid mode, providing both monitoring and access services

IDS Detection Types

The IDS attack detection has the following five types:

- DDoS attack detection, detecting DDoS attacks involving ARP, ICMP and SYN packets
- Flooding attack detection, detecting the flooding attacks involving single-user or multi-user management packets
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication attacks
- Weak IV attack detection, detecting weak vector attacks
- CMCC DoS attack detection

User Isolation Modes

The user isolation has the following five modes:

- AC-based: Communication cannot proceed between layer-2 users of different APs under the same AC.
- AP-based: Communication cannot proceed between layer-2 users under the same AP.
- AC-SSID based: Communication cannot proceed between layer-2 users of different APs under the same AC and in the same WLAN.
- AP-SSID based: Communication cannot proceed between layer-2 users under the same AP and in the same WLAN.
- SSID-based: Communication cannot proceed between layer-2 users in specified WLAN.

Rogue Containment Modes

The Rogue containment has the following four modes:

- Ad-hoc containment mode, containing the Rogue Ad-hoc devices
- Rogue containment mode, containing the Rogue devices with over-limit RSSI
- SSID containment mode, containing illegal devices with the same SSID
- Config containment mode, containing the illegal devices in the static attack list or the SSID blacklist

Fuzzy Containment on Rogue APs

- Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.

Detected Devices

The types of detected rogue devices are as follows:

- APs
- Ad-hoc devices
- Unknown STAs

Overview

Feature	Description

Frame filtering	Certain filtering rules are used to filter the packets from STAs for access control.
IDS	Timely discovers and defends against malicious or unintentional attacks in WLAN.
User isolation	Interdicts the insecure access between STAs in WLAN to prevent disclosure of private information.
Rogue detection and containment	Monitors abnormal devices in the whole WLAN, helping the network administrators find hidden dangers in networks. Rogue containment refers to containing Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices in a blacklist.

2.3.1 Frame Filtering

The access control over STAs includes: low-rate filter, whitelist, static blacklist, dynamic blacklist, SSID-based whitelist and SSID-based blacklist.

Working Principle

Low-Rate Filter

The low-rate filter sets a kickout threshold. When the threshold is larger than 0, the filter is enabled. If the STA rate is lower than this threshold, the STA's packets will be discarded and this STA will be disconnected.

Whitelist

The whitelist includes MAC addresses of admitted STAs. If the whitelist function is enabled, only the whistlisted can access the WLAN. Other STAs will be forced to go offline and cannot access the WLAN, so as to reduce the impact of illegal packets in the WLAN.

Static Blacklist

The static blacklist includes MAC address of the denied STAs. If the static blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access the network.

Dynamic Blacklist

The dynamic blacklist includes MAC addresses of the denied STAs. You can configure the dynamic blacklist if DDoS attacks are detected. For example, add the MAC address of a detected attacker into the blacklist dynamically to forbid receiving any packet from it, thereby ensuring WLAN security.

SSID-based Whitelist

The SSID-based whitelist includes MAC addresses of the STAs admitted into a WLAN with a specified SSID. You can configure the SSID-based whitelist. If the SSID-based whitelist function is enabled, only the STAs in the whitelist of the specified WLAN are allowed to access. Other STAs cannot access the specified WLAN and online STAs that are not in the whitelist will be forced to go offline, so as to reduce the impact of illegal packets in WLAN.

SSID-based Blacklist

The SSID-based blacklist includes MAC addresses of the STAs denied by a WLAN with a specified SSID. You can configure the SSID-based blacklist. If the SSID-based blacklist function is enabled, STAs in the blacklist will be forced to go offline and cannot access this WLAN.

2.3.2 IDS

In order to timely find and defend against malicious or unintentional attacks in WLAN, IDS supports the detection on multiple attacks. When an attack is detected, an alert or a log will be generated to remind the network administrator of treatment. Based on detected results, the network administrator can timely adjust network configuration to clear the insecure factors in WLAN.

Currently, our devices support the following types of IDS attack detection:

- DDoS attack detection
- Flooding attack detection
- Spoofing attack detection
- Weak IV detection
- CMCC DoS attack detection

Working Principle

↘ DDoS Attack Detection

DDoS attack means that the attackers send a large number of attack packets toward targeted devices in a short period of time (ARP packets, ICMP packets and SYN packets identified currently) so as to affect legal STAs being associated with the attacked device.

DDoS detection function performs statistics for the attacker's packets and determines whether the number of packets per second exceeds the configured threshold. If yes, this result will be logged. If the dynamic blacklist function is enabled, the attacker will be added into the dynamic blacklist.

↘ Flooding Attack Detection

Flooding attack refers to that an attacker sends a large number of packets of the same type in a short period of time, causing the WLAN devices fail to process legal STA requests due to the Rogue flooding.

Flooding attack detection prevents this flooding attack by continuously monitoring the traffic of each device. Within specified time, when the traffic exceeds the upper limit set by the network administrator, this device is deemed to be a flooding attacker and is therefore blocked. Flooding attack detection can be used with the dynamic blacklist function. When attacks are detected, if the dynamic blacklist function is enabled, the STA initiating the attacks will be added into the dynamic blacklist, ensuring no more intrusion by this STA and thus guaranteeing network security.

↘ Spoofing Attack Detection

Spoofing attack refers to that an attacker sends fake packets in the name of another STA. For example, a fake deauthentication packet causes a STA offline.

WIDS performs detection on the broadcast deauthentication and broadcast disassociation packets. When such packet is received, it is immediately defined as a spoofing attack and logged.

Weak IV Attack Detection

Weak IV (Weak Initialization Vector) attack refers to the following attack behavior: when the WLAN uses WEP encryption, an attacker intercepts packets with weak initialization vectors, cracks the shared key and finally steals the encrypted information.

When WLAN uses WEP for encryption, an initialization vector (IV) is generated for each packet and, together with the shared key, taken as input to generate a key string. With the key string and plain-text encryption, the cipher text is generated finally. When a WEP packet is sent, the IV used for packet encryption is also taken as a part of the packet header to be sent. If the IV is generated with an insecure method, for example, repetitive IVs are frequently generated or even the same IV is always generated, the shared key will be exposed easily. If a potential attacker obtains the shared key, it can control network resources and pose a threat to network security.

The IDS prevents this attack by identifying the IV of each WEP packet. When a packet with a weak IV is detected, the IDS immediately determines that this is vulnerability and logs this detected result.

CCMC DoS Attack Detection

The CMCC DoS attack detection refers to that for every STA which is connected or tries to access, if the number of Action, Association, Authentication, Deauthentication, Disassociation, Reassociation, Probe Request or Null data packets is larger than the set threshold, an attack is deemed existing.

2.3.3 User Isolation

Because of the mobility and uncertainty of STAs, STA information privacy appears to be particularly important in some occasions (especially public areas). Therefore, direct STA communication should be restricted. The user isolation technology can avoid insecure access between STAs in WLAN coverage (e.g., via online neighborhood), so as to prevent private information from being stolen by others.

User isolation isolates STAs, and prevents them from accessing each other without affecting their normal network access, guaranteeing service security. The layer-2 user isolation has the following five types:

- AP-based user isolation
- AP-SSID based user isolation
- AC-based user isolation
- AC-SSID based user isolation
- CMCC user isolation

Working Principle

AP-Based User Isolation

Direct communication cannot be conducted between layer-2 STAs associated with the same AP.

AP-SSID based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AP.

AC-based User Isolation

Direct communication cannot be conducted between layer-2 STAs who are associated with the same AC but with different APs. This is effective only in centralized forwarding mode.

AC-SSID based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AC but with different APs. This is effective only in centralized forwarding mode.

CMCC User Isolation

CMCC user isolation depends on SSID-based isolation functions. It takes effect on the APs in local forwarding mode and on ACs in centralized forwarding mode.

2.3.4 Rogue Detection and Containment

Network devices are usually divided into two types: illegal (Rogue) and legal. Rogue devices have potential vulnerabilities to be attacked or manipulated, which therefore poses a serious threat or hazard to network security. Rogue detection function can monitor abnormal devices in the whole WLAN, helping the network administrator find hidden dangers in networks.

Rogue detection is applicable to multiple Rogue devices in WLAN: APs, clients, wireless bridges, and Ad-hoc devices. Currently, only the detection on Rogue APs and Ad-hoc devices and unknown STAs is supported.

Rogue device containment counters Rogue devices by sending fake deauthentication frames to the addresses of Rogue devices, as so to prevent STAs from accessing illegal service or illegal STAs from accessing the devices.

Working Principle

Rogue Detection

The Rogue detection function is conducted by an AP in Monitor mode or Hybrid mode. WIDS captures wireless packets in the air by deploying some APs in WLAN and setting them to operate in Monitor or Hybrid mode. By conducting analysis and statistics of monitored wireless packets, the AP can obtain information on the Rogue device. Meanwhile, the network administrator can also prepare illegal device detection rules to monitor abnormal devices in the whole WLAN.

Unknown STA Detection

The unknown STA detection function monitors the probe request packets from non-accessed STAs in the network, and the network administrator can also use configuration to specify information on the unknown STA.

Rogue Containment

The Rogue containment refers to a service which uses the means of simulating fake broadcast deauthentication packets to contain Rogue devices that meet the containment mode rules, and to prevent normal STAs from accessing Rogue devices.

Unknown STA Containment

The unknown STA containment refers to denying unknown STA access by directly constructing deauthentication packets.

CMCC Rogue Detection

The function of CMCC Rogue detection is aimed at preventing illegal APs from interfering with legal APs in signal transmission, and even preventing legal STAs from being cheated out of registration information. Based on Rogue detection function, CMCC Rogue detection cuts off the network connection of illegal APs in collaboration with the background system, if conditions permit.

2.4 Configuration

Configuration	Description and Command	
Configuring Frame Filtering	(Optional) It is used to configure frame filtering.	
	kickout threshold	Configures the low-rate kickout threshold.
	whitelist mac-address [**name** *another-name*]	Adds an entry to the whitelist.
	whitelist max	Configures the length of the whitelist.
	static-blacklist mac-address [**name** *another-name*]	Adds an entry to the static blacklist.
	static-blacklist max	Configures the length of the static blacklist.
	dynamic-blacklist enable	Enables the dynamic blacklist function.
	dynamic-blacklist lifetime	Configures the lifetime of the dynamic blacklist.
	dynamic-blacklist ac-max	Configures the length of the dynamic blacklist on ACs.
	dynamic-blacklist ap-max	Configures the length of the dynamic blacklist on APs.
	dynamic-blacklist mac-address [**name** *another-name*]	Adds an entry to the dynamic blacklist.
	ssid-filter max	Configures the SSID-based blacklist and whitelist and their length.
	ssid-filter blacklist mac-address [**name** *another-name*]	Adds an entry to the SSID-based blacklist.
	ssid-filter blacklist max	Configures the length of the SSID-based blacklist, 256 by default.
	ssid-filter whitelist mac-address	Adds an entry to the SSID-based whitelist.
	ssid-filter whitelist max	Configures the length of the SSID-based whitelist, 256 by default.
Configuring IDS	(Mandatory) It is used to configure IDS.	
	attack-detection enable	Specifies the IDS type.
	attack-detection ddos	Configures the interval and packet threshold of DDoS attack detection.

Configuration	Description and Command	
	attack-detection flood multi-mac	Configures the interval and packet threshold of multi-STA flooding attack detection.
	attack-detection flood single-mac	Configures the interval and packet threshold of single-user flood attack detection.
	attack-detection spoof	Configures the interval and packet threshold of the spoofing attack detection.
	attack-detection weak-iv	Configures the interval and packet threshold of the weak IV attack detection.
	attack-detection statistics ac-max	Configures the length of IDS statistics on ACs.
	attack-detection statistics ap-max	Configures the length of IDS statistics on APs.
	dos-detection	Configures CMCC DoS attack detection.
Configuring User Isolation	(Optional) It is used to configure user isolation.	
	user-isolation enable	Enables the AC-based, AP-based, AC-SSID-based, AP-SSID-based and CMCC layer-2 user isolation.
	user-isolation permit-mac	Adds an entry to the permissible MAC list for user isolation.
	user-isolation permit-mac max	Configures the length of the permissible MAC list for user isolation.
Configuring Rogue Detection and Containment	(Optional) It is used to set the device detection and containment function.	
	countermeasures enable	Enables the Rogue containment function.
	countermeasures ap-max	Configures the maximum number of contained devices once.
	countermeasures channel-match	Enables channel-based containment.
	countermeasures interval	Configures the containment interval.
	countermeasures mode	Configures the containment mode.
	countermeasures rssi-min	Configures the minimum containment RSSI.
	countermeasures fuzzy-enable	Enables fuzzy containment.
	device aging duration	Configures the aging duration of the detected devices.
	device attack mac-address	Adds an entry to the static attack list.
	device attack max	Configures the length of the static attack list.
	device black-ssid	Adds an entry to the SSID-based blacklist.
	device max-black-ssid	Configures the length of the SSID-based blacklist.
	device friendly-flags	Configures the device friendly flag.
	device permit mac-address	Adds an entry to the permissible MAC list.
	device permit mac-address max	Configures the length of the permissible MAC list.
	device permit ssid	Adds an entry to the permissible SSID list.
	device permit max-ssid	Configures the length of the permissible SSID list.

Configuration	Description and Command	
	device permit vendor bssid	Adds an entry to the permissible vendor list.
	device permit vendor bssid max	Configures the length of the permissible vendor list.
	device unknown-sta dynamic-enable	Enables unknown STA detection and containment.
	device unknown-sta mac-address	Adds an entry to the unknown STA list
	device unknown-sta mac-address max	Configures the length of the unknown STA list.
	device unknown-sta report enable	Enables unknown STA detection information reporting.
	device channel-bind radio	Configures the scanning channel of a specified radio.
	device scan-para	Configures the CMCC illegal AP detection.
	device detected-ap-max	Configures the maximum number of detected APs.
	hybrid-scan radio	Configures the scanning status of a specified radio.
	scan-channels { 802.11a | 802.11b } channels	Configures the scanning channel of a specified AP.
	scan-channels dual-band	Configures automatic channel scanning between different frequency bands.
	rogue-ap countermeasures enable	Enables CMCC Rogue containment.
configuring AP Working Modes	(Optional) It is used to set the AP working mode.	
	device mode	Configures the AP working mode.

2.4.1 Configuring Frame Filtering

Configuration Effect

- Configure the frame filtering rules to provide packet filtering services.

Notes

- An STA cannot be configured in both the static blacklist and the whitelist.
- An STA cannot exist in both the blacklist and whitelist of the same SSID.

Configuration Steps

Configuring the Low-Rate Filter

- (Optional) The **kickout threshold** command is used in WIDS configuration mode to configure the low-rate kickout threshold. The low-rate filtering function effectively works only after the low-rate kickout threshold is configured (larger than 0).
- Unless otherwise noted, enable this function only on ACs which needs to support the low-rate STA filtering function.

Command	**kickout threshold** *rate*
Parameter Description	*rate*: Indicates the low-rate kickout threshold ranging from 0 to 130 Mbps.
Defaults	By default, low-rate STAs are not filtered out, and the kickout threshold is 0.
Command Mode	WIDS configuration mode
Usage Guide	The STAs can select different low-rate STA filtering thresholds based on requirements.

Configuring the Whitelist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the whitelist function.
- To configure the whitelist entry, the same as above.
- To configure the whitelist length, the same as above.
- Run the **whitelist mac-address** command to add an entry to the whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **whitelist max** command to configure the maximum number of entries in the whitelist in WIDS configuration mode.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**whitelist** { **mac-address** *H.H.H* [**name** *another-name*] |**max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a whitelist entry. **name** *another-name*: Indicates the another-name of the MAC address in the whitelist. **max** *num*: Indicates the length of the whitelist ranging from 1 to 2,048.
Defaults	By default, the whitelist is empty and the whitelist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The whitelist function takes effect only when the whitelist has entries.

Configuring the Static Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the static blacklist function.
- To configure the static blacklist entry, the same as above.
- To configure the static blacklist length, the same as above.
- Run the **static-blacklist mac-address** command to add an entry to the static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **static-blacklist max** command to configure the maximum number of entries in the static list in WIDS configuration mode, indicating the maximum number of permissible static blacklist entries on the device.

- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**static-blacklist** { **mac-address** *H.H.H* [**name** *another-name*] | **max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static blacklist entry. **name** *another-name*: Indicates the another-name of the MAC address in the static blacklist. **max** *num*: Indicates the length of the static blacklist ranging from 1 to 2,048.
Defaults	By default, the static blacklist is empty and the static blacklist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The static blacklist function takes effect only when the static blacklist has entries.

Configuring the Dynamic Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the dynamic blacklist function.
- Run the **dynamic-blacklist enable** command to enable the dynamic blacklist function in WIDS configuration mode. A dynamic blacklist entry is generated dynamically along with the IDS attack detection and works only after the dynamic blacklist function is enabled.
- Run the **dynamic-blacklist lifetime** command to configure the service life of the dynamic blacklist in WIDS configuration mode, indicating how long the dynamic blacklist exists in the device.
- Run the **dynamic-blacklist** { **ac-max** | **ap-max** } command to configure the maximum number of dynamic blacklist entries on both ACs and APs in WIDS configuration mode.
- Run the **dynamic-blacklist mac-address** command to add an entry to the dynamic blacklist in WIDS configuration mode.

Command	**dynamic-blacklist** { **enable** | **lifetime** *time* |**ac-max** *num* |**ap-max** *num* | **mac-address** *H.H.H* }
Parameter Description	**enable**: Enables the dynamic blacklist function **lifetime** *time*: Indicates the service life of the dynamic blacklist ranging from 60 to 86,400 seconds. **ac-max** *num*: Indicates the length of the dynamic blacklist on ACs. **ac-max** *num*: Indicates the length of the dynamic blacklist on APs. **mac-address** *H.H.H*: Indicates the MAC address of a dynamic blacklist entry.
Defaults	By default, the dynamic blacklist function is disabled. The default length of the dynamic blacklist is 2,048 on ACs and APs with 300-second lifetime.
Command Mode	WIDS configuration mode
Usage Guide	A dynamic blacklist entry is generated in the IDS attack detection function.

Configuring the SSID-Based Blacklist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the SSID-based blacklist function.

- To configure the SSID-based blacklist entry, the same as above.
- To configure the SSID-based blacklist length, the same as above.
- To configure the SSID list length, the same as above.
- Run the **ssid-blacklist mac-address** command to add an entry to the SSID-based static blacklist in WIDS configuration mode. The static blacklist filtering function effectively works only after an effective static blacklist entry is configured.
- Run the **ssid-filter blacklist max** command to configure the maximum number of entries in the SSID-based static blacklist in WIDS configuration mode.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **blacklist max** *num* }
Parameter Description	**max** *num*: Indicates the maximum length of the SSID-based blacklist, ranging from 1 to 128. The default is 64. **blacklist mac-address** *H.H.H* **in-ssid** *string*: Adds an entry to the specified SSID-based blacklist. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID blacklist. **blacklist max** *num*: Configures the length of the SSID-based blacklist, ranging from 1 to 2048.
Defaults	The SSID-based blacklist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based blacklist has entries.

Configuring the SSID-Based Whitelist

- Optional.
- Unless otherwise noted, enable this function only on ACs which need the SSID-based whitelist function.
- To configure the SSID-based whitelist entry, the same as above.
- To configure the SSID-based whitelist length, the same as above.
- Run the **ssid-filter whitelist mac-address** command to add an entry to the SSID-based whitelist in WIDS configuration mode. The whitelist filtering function effectively works only after an effective whitelist entry is configured.
- Run the **ssid-filter whitelist max** command to configure the maximum number of entries in the SSID-based whitelist in WIDS configuration mode.
- One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name.
- The another-name is null if it is not configured.

Command	**ssid-filter** { **whitelist mac-address** *H.H.H* [**name** *another-name*] **in-ssid** *string* | **whitelist max** *num* }
Parameter Description	**whitelist mac-address** *H.H.H* **in-ssid** *string*: Configures the whitelist entry for a specified SSID. **name** *another-name*: Indicates the another-name of the MAC address in the specified SSID whitelist. **whitelist max** *num*: Configures the length of the SSID-based whitelist, ranging from 1 to 2048.

Defaults	The SSID-based whitelist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based whitelist has entries.

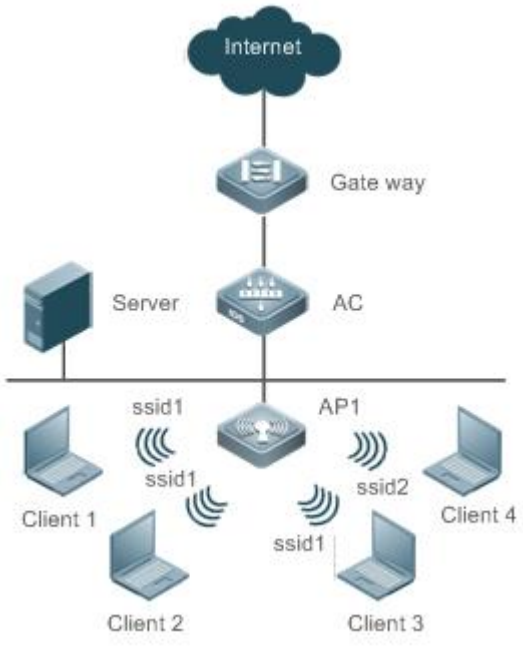
Verification

Conduct related function verifications based on corresponding frame filtering rules.

- Check the low-rate STA filtering function. The packets are discarded and the low-rate STAs are successfully removed.
- Check the whitelist function. When the whitelist is configured, the STAs not included in the whitelist cannot join the AP.
- Check the static blacklist function. When the static blacklist is configured, the STAs included in the static blacklist cannot join the AP.
- Check the dynamic blacklist function. When the dynamic blacklist function is enabled, entries in the dynamic blacklist can be generated along with the IDS attack detection, and STAs in the dynamic blacklist cannot join the AP again.
- Check the SSID-based blacklist function. When the SSID-based blacklist is configured, STAs in the SSID-based blacklist cannot join this SSID service.
- Check the SSID-based whitelist function. When the SSID-based whitelist is configured, STAs not included in the SSID-based whitelist cannot join this SSID service.

Configuration Example

Configuring the Whitelist Entry

Scenario **Figure 2-5**	
Configuration Steps	● Add an entry to thewhitelist on the AC.

	Ruijie# configure terminal Ruijie(config)# wids Ruijie(config-wids)# whitelist mac-address 0000.0000.0001
Verification	After the STA configures the whitelist entry, the following methods can be used to check the configuration. ● Run the **show wids whitelist** command to display the information on related parameters configured onthe STA. ● Use the device to verify whether the function has taken effect.
	Ruijie#show wids whitelist ------------------ Whitelist Information ------------------ num Mac-address 1 0000.0000.0001

Common Errors

N/A

2.4.2 Configuring IDS

Configuration Effect

- IDS can be used to timely find and defend against malicious or unintentional attacks in WLAN.

Notes

- IDS needs to be used together with the dynamic blacklist function, to effectively prevent attacks against WLAN.

Configuration Steps

↘ Specifying the IDS Type

- (Optional) IDS is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the IDS attack detection function.
- To configure the IDS attack detection, the same as above.

Command	**attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }
Parameter Description	**ddos**: Enables DDoS attack detection. **flood**: Enables flooding attack detection. **spoof**: Enables spoofing attack detection. **weak-iv**: Enables Weak IV attack detection. **all**: Enables all IDS attack detection.
Defaults	All IDS attack detection is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring DDoS Attack Detection

- Optional.
- Unless otherwise noted, configure this function on ACs which need DDoS attack detection.
- To configure the thresholds and intervals of a specified type of packets in DDoS attack detection, the same as above.

Command	**attack-detection ddos** { **arp-threshold** *num*| **icmp-threshold** *num*| **syn-threshold** *num* | **interval** *time* }
Parameter Description	**arp-threshold** *num*: Indicates ARP packet threshold ranging from1 to 10,000 pps. **icmp-threshold** *num*: Indicates ICMP packet threshold ranging from110,000 pps. **syn-threshold** *num*: Indicates SYN packet threshold ranging from1 to 10,000 pps. **interval** *time*: Indicates the period of DDoS attack detection ranging from 10 to 60 seconds.
Defaults	By default, the interval of DDoS attack detection is 30 seconds, and the three DDoS attack detection thresholds are 50 pps for ARP packets, 100 pps for ICMP packets, and 50 pps for SYN packets.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Flooding Attack Detection

- (Optional) Flooding attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the flooding attack detection.
- To configure the threshold and interval of a specified types of packets in flooding attack detection, the same as above.
- Run the **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold***num***interval***time* command to configure the threshold and interval of a specified type of packets for single-STAflooding attack in WIDS configuration mode.
- Run the **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* command to configure the threshold and interval of a specified type of packets for multi-STA flooding attack in WIDS configuration mode.

Command	**attack-detection flood single-mac** { **total**	**assoc**	**reassoc**	**disassoc**	**probe**	**action**	**auth**	**deauth |** **null-data** } **threshold** *num* **interval** *time*
Parameter Description	**single-mac**: Indicates single STA detection. **total**: Indicates all packets. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 10000.

	time: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4800 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Command	**attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*
Parameter Description	**multi-mac**: Indicates multi-STA detection. **assoc**: Indicates Association packets. **reassoc**: Indicates Reassociation packets. **disassoc**: Indicates Disassociation packets. **probe**: Indicates Probe packets. **action**: Indicates Action packets. **auth**: Indicates Authentication packets. **deauth**: Indicates Deauthentication packets. **null-data**: Indicates Null packets. *num*: Indicates the packet threshold of flooding attack detection ranging from 1 to 10000. *time*: Indicates the interval of flooding attack detection ranging from 10 to 60 seconds.
Defaults	All packet thresholds of flooding attack detection, by default, 300 for single-STA, 4800 for multi-STA, and 10 seconds of the statistic interval
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Spoofing Attack Detection

- (Optional) Spoofing attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the spoofing attack detection.
- To configure the threshold and interval of a specified type of packets in spoofing attack detection, the same as above.

Command	**attack-detection spoof** { **threshold** *num* |**interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet threshold of spoofing attack detection ranging from 1 to 1,000. **interval** *time*: Indicates the interval of spoofing attack detection ranging from 10 to 60 seconds.
Defaults	By default, the packet threshold is 1 and the detection interval is 50 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Weak IV Attack Detection

- (Optional) The Weak IV attack detection function is disabled by default.
- Unless otherwise noted, configure this function on ACs which needs the Weak IV attack detection.
- To configure the thresholds and intervals for specified types of packets in Weak IV attack detection, the same as above.

Command	**attack-detection weak-iv** { **threshold** *num*| **interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet threshold of weak IV attack detection ranging from 1 to 10,000. **interval** *time*: Indicates the interval of weak IV attack detection ranging from 1 to 60 seconds.
Defaults	The default interval of Weak IV detection is 15 seconds, and the default detection threshold is 10.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring CMCC DoS Attack Detection

- (Optional) CMCC DoS attack detection is disabled by default.
- Unless otherwise noted, configure this function on ACs which need the Weak IV attack detection.
- To configure the threshold and interval of a specified type of packets in CMCC DoS attack detection, the same as above.

Command	**dos-detection** { **enable** | **threshold** *num*| **interval** *time* }
Parameter Description	**enable:** Enables CMCC DoS attack detection **threshold** *num*: Indicates the packet threshold of CMCC DoS attack detection ranging from 1 to 5,000. **interval** *time*: Indicates the interval of the CMCC DoS attack detection ranging from 1,000 to 60,000 ms.
Defaults	The interval of CMCC DoS attack detection is 1,000 ms, and the detection threshold is 30.
Command Mode	WIDS configuration mode
Usage Guide	N/A

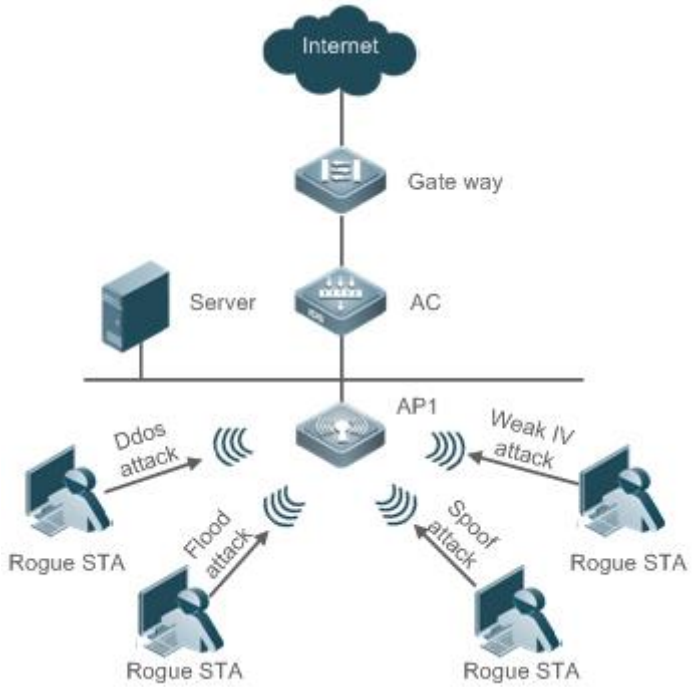
Verification

Carry out related verifications based on the IDS attack detection type:

- DDoS attack detection, detecting the ARP packet attack, ICMP packet attack and SYN packet attack.
- Flooding attack detection, detecting the multi-STA flooding attack and single-STA flooding attack.
- Spoofing attack detection, detecting the broadcast disassociation and deauthentication packet attacks.
- Weak IV attack detection, detecting the weak IV packet attack.
- CMCC DoS attack detection, detecting the DoS attack.

Configuration Example

Configuring DDoS Attack Detection

Scenario **Figure 2-6**	
Configuration Steps	● Specify the IDS type and configure related thresholds on the AC.
	`Ruijie# configure terminal` `Ruijie(config)# wids` `Ruijie(config-wids)# attack-detection enable flood` `Ruijie(config-wids)# attack-detection ddos interval 10`
Verification	● If a DDoS attack exists, related syslog information will be printed on the AC.
	`*Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ARP DDOS attack to Ap (1414.0902.0016).` `Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): ICMP DDOS attack to Ap (1414.0902.0016).` `Feb 7 13:37:03: %WIDS-6-ATTACK: Client(0025.64b8.2ffa): SYN DDOS attack to Ap (1414.0902.0016).`

Common Errors

N/A

2.4.3 Configuring User Isolation

Configuration Effect

- After user isolation is configured, direct communication cannot be conducted between STAs meeting the user isolation rules.

Notes

- User isolation is only valid for layer-2STAs.

Configuration Steps

Configuring the User Isolation Mode

- Optional.
- Unless otherwise noted, configure this function on ACs.

Command	**user-isolation** { **ac** | **ap** | **ssid-ac** | **ssid-ap** | **wlan-id** *num* } **enable**
Parameter Description	**ac:** Indicates AC-based layer-2 user isolation. **ap:** Indicates AP-based layer-2 user isolation. **ssid-ac:** Indicates AC-SSID-based layer-2 user isolation. **ssid-ap:** Indicates AP-SSID-based layer-2 user isolation. **wlan-id** *num*: Indicates SSID-based layer-2 user isolation.
Defaults	User isolation is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The AC-based and AC-SSID-based layer-2 user isolation are effective only in centralized forwarding mode.

Configuring the Permissible MAC List for User Isolation

- Optional.
- Unless otherwise noted, configure this information on ACs.
- To configure the isolation list length, the same as above.

Command	**user-isolation permit-mac** {*H.H.H* | **max** *num* }
Parameter Description	*H.H.H*: Indicates the permissible MAC list entry for user isolation. **max** *num*: Indicates the permissible MAC list length for user isolation ranging from 1 to 1,024.
Defaults	The permissible STA's MAC list for isolation is empty, with the default length of 1,024.
Command Mode	WIDS configuration mode
Usage Guide	N/A

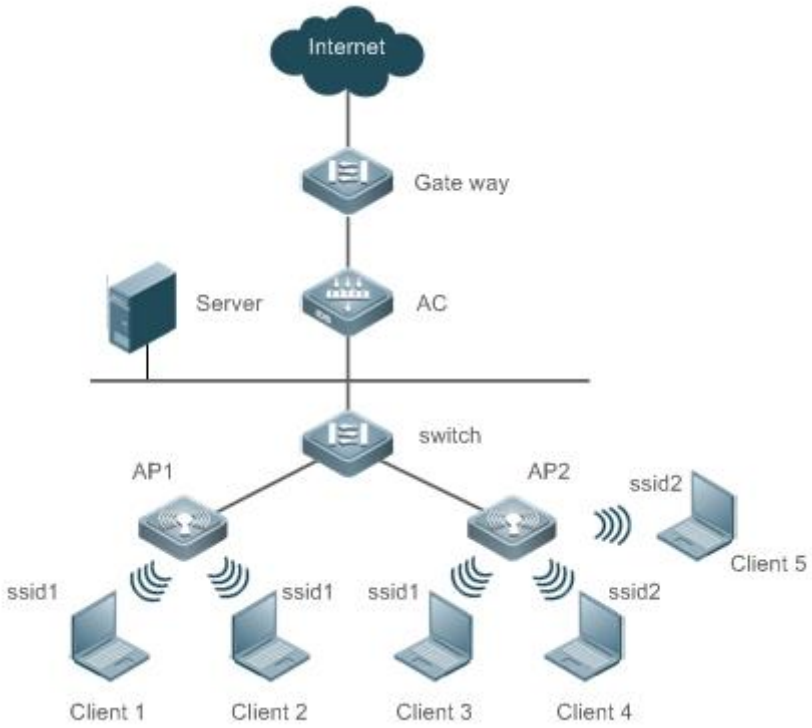
Verification

- Carry out related verifications based on the isolation mode.

Configuration Example

Configuring User Isolation

Scenario	

Figure 2-7	
Configuration Steps	● Configure the AP-based layer-2 user isolation on the AC.
	`Ruijie# configure terminal` `Ruijie(config)# wids` `Ruijie(config-wids)# user-isolation ap enable`
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA.
	`Ruijie#show running-config` `…` `!` `wids` ` user-isolation ap enable` `!`

Common Errors

N/A

2.4.4 Configuring Rogue Detection and Containment

Configuration Effect

Configure Rogue detection and containment provide illegal device suppression and maintain WLAN security.

Notes

The detection and containment of Rogue devices takes effect only when the AP working mode is Hybrid or Monitor.

Configuration Steps

Enabling Rogue Containment

- Optional. Run the **countermeasures enable** command to enable Rogue containment in WIDS configuration mode.
- Unless otherwise noted, this function is configured on ACs which need the Rogue containment function.

Command	**countermeasures enable**
Parameter Description	N/A
Defaults	Rogue containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Interval

- Optional. Run the **countermeasures interval** *time* command to configure the interval of Rogue containment in WIDS configuration mode.
- Unless otherwise noted, configure the containment interval on ACs which need the Rogue device containment period.

Command	**countermeasures interval** *time*
Parameter Description	time: Indicates the containment interval ranging from 100 to 10,000 ms.
Defaults	The default containment interval is 1,000 ms.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Containment Mode

- Optional. Run the **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** } command to configure the Rogue containment mode in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need Rogue containment mode.

Command	**countermeasures mode** { **all**	**adhoc**	**config**	**rogue**	**ssid** }
Parameter Description	**adhoc**: Indicates Ad-hoc containment mode, countering Ad-hoc devices. **config**: Indicates Config containment mode, countering devices which meet entries in the SSID blacklist and static attack list. **rogue**: Indicates Rogue containment mode, countering devices whose RSSI is larger than the threshold. **ssid**: Indicates SSID containment mode, countering devices with the same SSID but not on the same AC. **all**: Indicates all the above containment modes.

Defaults	No containment mode is specified by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Static Attack List

- Optional. Run the **device attack mac-address** *H.H.H* command to configure the static attack statistic list information in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the static attack list.

Command	**device attack** { **mac-address** *H.H.H* |**max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the MAC address of a static attack list entry. **max** *num*: Indicates the length of the static attack list, ranging from 1 to 1,024.
Defaults	The static attack list is empty, and the length of the static attack list is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the SSID-based Blacklist

- Optional. Run the **device black-ssid** *ssid* command to configure the SSID blacklist information in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the SSID blacklist.

Command	**device { black-ssid** *ssid* |**max-black-ssid** *num* }
Parameter Description	**black-ssid** ssid: Indicates the SSID blacklist entry. **max-black-ssid** *num*: Indicates the SSID blacklist length, ranging from 1 to 1,024.
Defaults	The SSID blacklist is empty, and the SSID blacklist length is 512 by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Lists of Permissible MACs, SSIDs and Vendors

- Optional.
- Unless otherwise noted, configure these on ACs which need the permissible MAC, permissible SSID and permissible vendor lists.
- Run the **device permit mac-address** *H.H.H* command to configure the permissible MAC list entry in WIDS configuration mode.
- Run the **device permit ssid** *H.H.H* command to configure the permissible SSID list entry in WIDS configuration mode.
- Run the **device permit vendor** *H.H.H* command to configure the permissible vendor list entry in WIDS configuration mode.

Command	**device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }
Parameter Description	**mac-address** *H.H.H*: Indicates the permissible MAC list entry, null by default. **mac-address max** *num*: Indicates the permissible MAC list length, ranging from 1 to 2,048, 1,024 by default. **ssid** *ssid*: Indicates the permissible SSID list entry, null by default. **max-ssid** *num*: Indicates the permissible SSID list length, ranging from 1 to 1,024, 512 by default. **vendor bssid** *H.H.H*: Indicates the permissible vendor list entry, null by default. **vendor bssid max** *num*: Indicates the permissible vendor list length, ranging from 1 to 1,024, 512 by default.
Defaults	See the **Parameter Description**.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Maximum Number of Contained Devices Once

- Optional. Run the **countermeasures ap-max** *ap-num* command to configure the quantity of one-time Rogue device containment in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need to configure the contained Rogue device quantity.

Command	**countermeasures ap-max** *ap-num*
Parameter Description	*ap-num*: Indicates the maximum number of countered devices each time, ranging from 1 to 256.
Defaults	The default maximum number of countered devices is 30.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Aging Duration of the Detected Devices

- Optional. Run the **device aging duration** *time* command to configure the aging duration of the detected devices in WIDS configuration mode.
- Unless otherwise noted, configure this on ACs which need the aging time.

Command	**device aging duration** *time*
Parameter Description	*time*: Indicates the aging duration, ranging from 500 to 5,000 seconds.
Defaults	The default aging duration is 1,200 seconds.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Device Friendly Flag

- Optional. Run the **device friendly-flags** *value* command to configure the device friendly flag in WIDS configuration mode. With the device friendly flag, the AP device can identify devices on the same AC.
- Unless otherwise noted, configure this on ACs which need the device friendly flag.

Command	**device friendly-flags***value*
Parameter Description	*value*: Indicates the device friendly flag, ranging from 1 to 4294967295.
Defaults	The default value is 0.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring the Minimum Containment RSSI

- Optional. Run the **countermeasures rssi-min** *num* command to configure the minimum containment RSSI in WIDS configuration mode. A Rogue device which exceeds this RSSI will be countered.
- Unless otherwise noted, configure this on ACs which need logs to be written into the memory buffer.

Command	**countermeasures rssi-min** *num*
Parameter Description	*num*: Indicates the minimum containment RSSI, ranging from 0 to 75 (-95 to -20).
Defaults	The default minimum containment RSSI is 25 (-70) by default.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Channel-Based Containment

- Optional. Run the **countermeasures channel-match** command to enable channel-based containment function in WIDS configuration mode. The channel-based containment can be conducted based on the channel on which the detected Rough device operates.
- Unless otherwise noted, configure this on ACs which need the channel-based containment function.

Command	**countermeasures channel-match**
Parameter Description	**channel-match**: Enables channel-based containment.
Defaults	Channel-based containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Configuring Fuzzy Containment

- Optional. Run the **countermeasures fuzzy-enable** command to configure the fuzzy containment function in WIDS configuration mode. Fuzzy match is performed based on the SSID of the rogue AP. For example, if the SSID of the local

host is RUIJIE-WEB, the rogue AP whose SSID is RU1JIE-WEB can be contained after the fuzzy containment function is enabled.

- Unless otherwise specified, configure the fuzzy containment function on ACs which require this function.

Command	**countermeasures fuzzy-enable**
Parameter Description	N/A
Defaults	The fuzzy containment function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	If containment modes include the configuration containment mode, rogue APs whose SSID are similar to those in the SSID blacklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local host are contained. Fuzzy containment takes effect only in configuration containment mode and SSID containment mode.

Enabling Unknown STA Detection and Containment

- Optional.
- Unless otherwise noted, configure this on ACs which need the unknown STA detection and containment function.
- Run the **device unknown-sta dynamic-enable** command to enable the unknown STA detection and containment function in WIDS configuration mode.
- Run the **device unknown-sta mac-address** *H.H.H* command to configure the unknown STA list entry in WIDS configuration mode.

Command	**device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }
Parameter Description	**dynamic-enable**: Enables unknown STA detection and containment. **mac-address** *H.H.H*: Configures the unknown STA list entry, empty by default. **mac-address max** *num*: Configures the unknown STA list length, ranging from 1 to 256.
Defaults	Unknown STA detection and containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function has no effect when the AP operates in Normal mode.

Enabling Unknown STA Detection Information Reporting

- Optional.
- This command is used to report detected unknown STAs to the AC.
- Run the **device unknown-sta report enable** command to enable the unknown STA detection information reporting function in WIDS configuration mode.

Command	**device unknown-sta report enable**
Parameter Description	N/A

Defaults	The unknown STA detection information reporting function is disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the AP does not operate in Normal mode. The scanning result can be reported to the AC.

Configuring CMCC Rogue Detection

- Optional.
- Unless otherwise noted, configure these on ACs which need the function of CMCC Rogue detection.
- Run the **device channel-bind radio** *radio-id* { **channel** *num*| **max-cycles** *value* } command to configure the scanning channel of a specified radio for CMCC Rogue detection in AP configuration mode.
- Run the **device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* } command to configure the scanning parameters for detection of interoperability with illegal APs in AP configuration mode.
- Run the **rogue-ap countermeasures enable** command to configure the function of containing interoperability with illegal APs in WIDS configuration mode.
- Configure the scanning channel information on interoperability with illegal APs

Command	**device channel-bind radio** *radio-id*{ **channel** *num* | **max-cycles** *value* }
Parameter Description	*radio-id*: Indicates Radio ID of a specified AP. **channel** *num*: Channel value, Chinese channel by default. **max-cycles** *value*: indicates the number of scanning times, 10 by default and ranging from 0 to 255.
Defaults	For details, see the **Parameter Description**.
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } **|** **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }
Parameter Description	**radio** *radio-id*: Radio ID **scan-type active**: Indicates active scanning. The default scanning is passive scanning. **scan-type passive**: Indicates passive scanning. **device-detect enable**: Enables the detection. The detection is disabled by default. **device-detect disable**: Disables the detection. **ap-mode normal**: Indicates The AP works in Normal mode. **ap-mode monitor**: Indicates The AP works in Monitor mode. **detect-rpt-time** time: Indicates the detection reporting period, 60 seconds by default, ranging from 60 to 120 seconds.
Defaults	For defaults, see the **Parameter Description**.

Command Mode	AP configuration mode
Usage Guide	N/A

Command	**rogue-ap countermeasures enable**
Parameter Description	N/A
Defaults	Disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Detected APs

- Optional. Run the **device detected-ap-max** *num* command to configure the maximum number of detected APs in WIDS configuration mode. A smaller configuration value leads to less data being detected on the AP. If less data is detected, the device containment function may not show an obvious containment effect. A larger configuration value requires more memory.
- Unless otherwise noted, configure this on ACs which need the maximum number of detected APs.

Command	**device detected-ap-max** *num*
Parameter Description	*num*: Indicates the maximum number of detected APs, ranging from 1 to 4,096.
Defaults	The default maximum number is 2,048.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Scanning Status of a Specified Radio

- Optional. Run the **hybrid-scan radio** *num* **{ disable | enable }** command to configure the scanning status of a specified radio in AP configuration mode. If disabling the configuration leads to AP working in non-normal mode, there will be no device detection data.
- Unless otherwise noted, configure this on ACs which need the radio scanning status.

Command	**hybrid-scan radio** *num* **{ enable	disable }**
Parameter Description	*num*: Indicates a radio ID.
Defaults	All radio scanning is enabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Scanning Channel of a Specified AP

- Optional. Run the **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13* command to configure the scanning channel in AP configuration mode. If the scanning channel is not configured, there will be no device detection data when the AP operates not in Normal mode.
- Unless otherwise noted, configure this on ACs which need the specified AP scanning channel.

Command	**scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13*
Parameter Description	*num*: Indicates a channel number.
Defaults	The scanning channel is null.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Automatic Channel Scanning Between Different Frequency Bands

- Optional. Run the **scan-channels dual-band radio** *radio-id* command to perform automatic channel scanning between two frequency bands, to obtain the scanning result of the two frequency bands and perform containment.

Command	**scan-channels dual-band radio** *radio-id*
Parameter Description	*radio-id*: Indicates the radio ID of the AP for which automatic channel scanning between different frequency bands is enabled.
Defaults	Automatic channel scanning between different frequency bands is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The RF modules of partial APs support both the 2.4 GHz and 5 GHz frequency bands. When the RF modules are used for channel scanning, this command can be used for automatic channel scanning between the two frequency bands, to obtain the scanning results of these two frequency bands and perform containment. After the frequency bands are switched, channels configured by running the **scan-channels { 802.11a | 802.11b } channels** command are scanned. In addition, for some APs that have channel restrictions, the restricted channels will be automatically skipped during channel scanning.

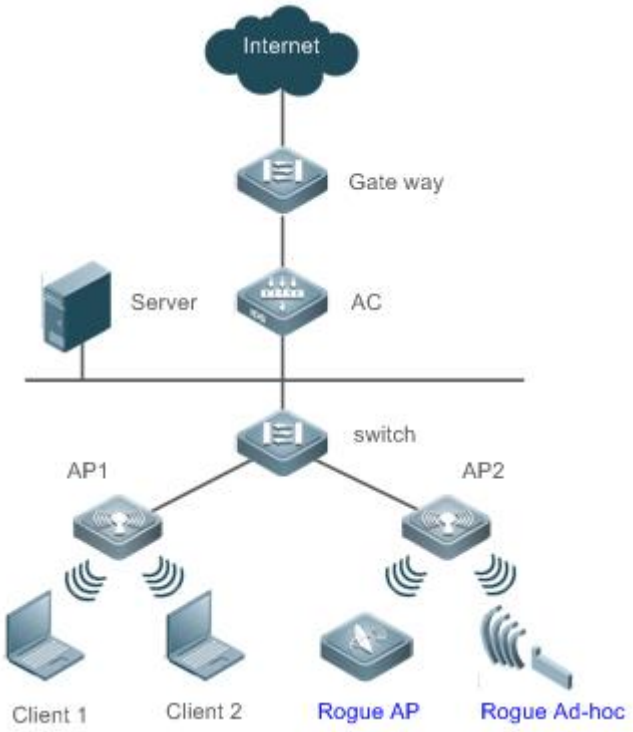
Verification

- Run the **show wids detected** command to display the detected results.

Configuration Example

Configuring Rogue Containment

Scenario	

Figure 2-8	
Configuration Steps	● Configure Rogue containment information on the AC. Before configuring containment, confirm that the WLAN service has been deployed on the contained AP; otherwise, the containment will not take effect.
	`Ruijie# configure terminal` `Ruijie(config)# wids` `Ruijie(config-wids)# countermeasures enable` `Ruijie(config-wids)# countermeasures mode ssid`
Verification	● Run the **show running-config** command to display the information on related parameters configured by the STA and the log information generated by the system recently.
	`Ruijie#show running-config` `Ruijie#show running-config` `…` `!` `wids` ` countermeasures enable` ` countermeasures mode SSID` `!` `…`

Common Errors

N/A

2.4.5 Configuring AP Working Mode

Configuration Effect

- Based on the configured working mode, the AP can provide different services.

Notes

N/A

Configuration Steps

Configuring AP Working Modes

- Optional.
- Unless otherwise noted, configure this on each AP.

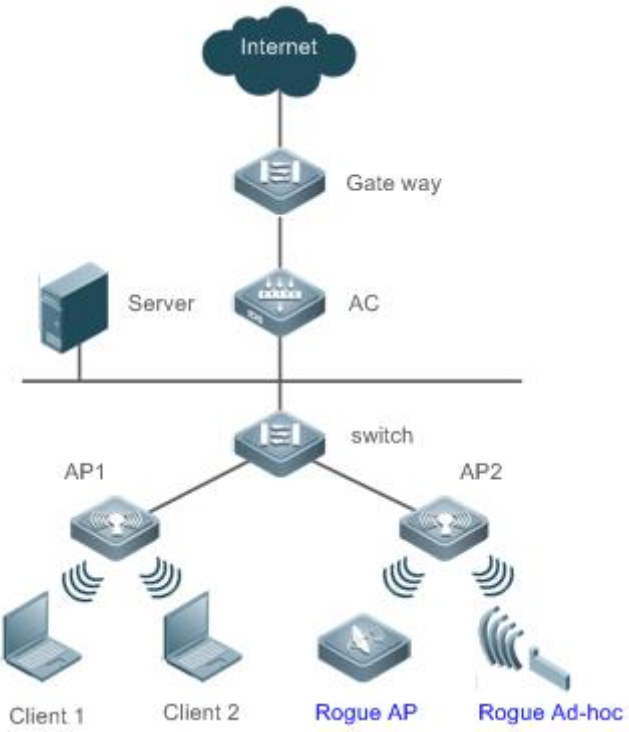
Command	**device mode** { **hybrid** | **monitor** | **normal** } [**radio** *radio-id*]
Parameter Description	**hybrid**: Indicates Hybrid mode, in which the device provides both monitoring service and access service. **monitor:** Indicates Monitor mode, in which the device provides only the monitoring service. **normal**: Indicates Normal mode, in which the device provides only the access service. **radio**: Specifies a radio to provide the monitoring service, while other radios to provide the access service.
Defaults	The working mode of the AP is Normal.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** *ap-name* command to display the current working mode of the AP.

Configuration Example

Configuring the AP Working Mode

Scenario **Figure 2-9**	
Configuration Steps	● Configure the working mode of a specified AP on the AC.
	Ruijie# configure terminal Ruijie(config)# ap-config ap220 Ruijie (config-ap)#device mode hybrid
Verification	● Run the **show ap-config running** *ap-name* command to display the information on related parameters configured by the STA.
	Ruijie#show ap-config running ap220 ! ap-config ap220 device mode hybrid 11acsupport enable radio 1 11acsupport enable radio 2 802.11n mcs support 23 radio 1 802.11n mcs support 23 radio 2 802.11ac mcs support 29 radio 1 802.11ac mcs support 29 radio 2 antenna receive 7 radio 1 antenna receive 7 radio 2 antenna transmit 7 radio 1 antenna transmit 7 radio 2

	!

Common Errors

N/A

2.5 Monitoring

Displaying

Description	Command
Displays the attack list configuration.	**show wids attack-list**
Displays the dynamic or static blacklist configuration.	**show wids blacklist** { **dynamic** | **static** }
Displays the SSID-based blacklist configuration.	**show wids black-ssid**
Displays the information of detected devices of a specified type.	**show wids detected** { **adhoc** | **all** | **friendly ap** **|interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }
Displays the SSID-based blacklist and whitelist configuration.	**show wids ssid-filter** { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid string**] }
Displays the configuration of permissible MAC, permissible SSID and permissible vendor lists.	**show wids permitted** { **mac-address** | **ssid** | **vendor** }
Displays the IDS information.	**show wids statistics**
Displays the unknown STA list configuration.	**show wids unknown-sta**
Displays the permissible MAC entries for user isolation.	**show wids user-isolation permit-mac**
Displays the whitelist entries.	**show wids whitelist**
Displays other WIDS configuration.	**show running-config**
Displays the CMCC DoS detection information.	**show wids dos-detected**
Displays the CMCC Rogue detection information.	**show wids rogue-ap detected**

3 Configuring CPU Protect Policy

3.1 Overview

CPU Protect Policy (CPP) is a CPU protection policy.

Malicious attacks are often found in network environment. Network devices are occupied with counterfeited management and protocol packets and have no time to process real management and protocol packets. In this way, the attacks bring destructive impacts on device security and network stability. The CPP function protects CPU resources and important packets by means of packet identification and rate limiting.

Protocols and Standards

N/A

3.2 Applications

Application	Description
Rate Limiting	Limits the rate of specified packets.

3.2.1 Rate Limiting

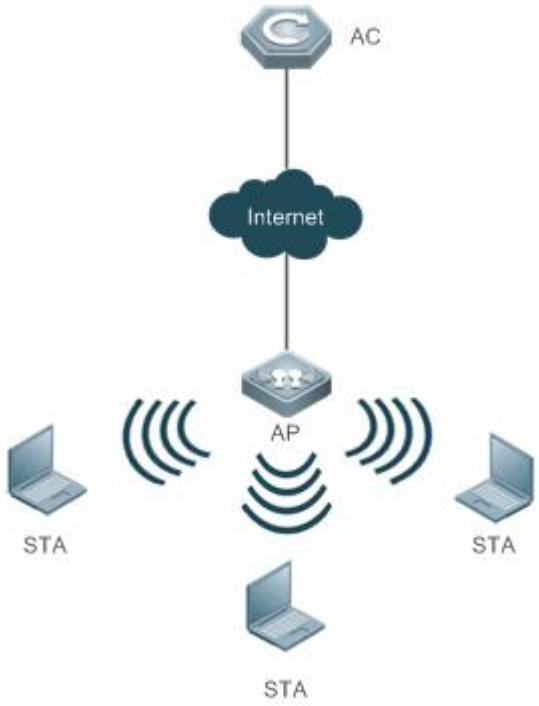
Scenario

The AC and AP are designed with the functions of packet identification and rate limiting, thus protecting the processors.

Figure 3-1 shows the networking topology of the CPP.

1. An AP accesses the AC.
2. Multiple STAs access the AP.
3. Specified packet attacks (see Configuration for details) may occur on STAs in a network. The AC and AP must be able to protect their CPU.

Figure 3-1 Networking Topology

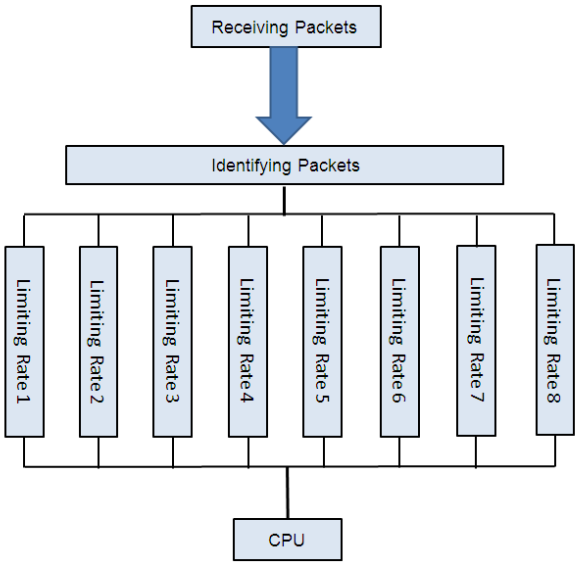


Deployment

- Apply the CPP function on the AC to limit the rate of specified packets.
- Apply the CPP function on the AP to limit the rate of specified packets.

3.3 Features

Figure 3-2 Working Principle



Basic Concepts

Identifying Packets

All packets that are sent to the AC/AP for protocol processing must be classified (e.g., into ARP, BPDU and d1x) through packet identification (for the data classification of different products, see Configuration).

Limiting Rate

An administrator can configure the rate limit for packets of each type, thus effectively dampening high-rate attack packets on the network.

Overview

Feature	Description
Identifying Packets	All packets that are sent to CPU are classified through packet identification.
Limiting Rate	High-rate attack packets are dampened by rate limiting.

3.3.1 Identifying Packets

All packets that are sent to CPU are classified through packet identification.

Working Principle

Identifying Packets

CPP classifies packets and automatically applies the packet identification function by default.

3.3.2 Limiting Rate

An administrator can configure the rate limit for packets of each type, thus effectively dampening high-rate attack packets on the network.

Working Principle

Limiting Rate

Packets that have been identified and classified are rate-limited, and packets that exceed the rate limit are discarded.

3.4 Configuration

Configuration	Description and Command	
Configuring the Rate Limit for Specified Packets	(Optional) It is used to set the rate limit for specified packets.	
	cpu-protect type	Sets the rate limit for specified packets
Configuring the Rate Limit for Wireless Management Packets	(Optional) It is used to set the rate limit for wireless management packets.	
	mgmt-ratelimit disable	Enables/disables the wireless management packet rate limiting function
	mgmt-ratelimit per-cti pps *value*	Configures the CTI-based rate limit for wireless management packets
	mgmt-ratelimit total pps *value*	Configures the AC-based rate limit for wireless management packets

3.4.1 Configuring the Rate Limit for Specified Packets

Configuration Effect

- Configure the rate limit for various types of packets.

Notes

N/A

Configuration Steps

Configuring the Rate limit for Specified Packets

- Optional.
- Enable the CPP function on all ACs/APs unless otherwise specified.
- A user can adjust the default rate limit for packets of each type according to actual requirements.

Command	**cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-realy-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng**

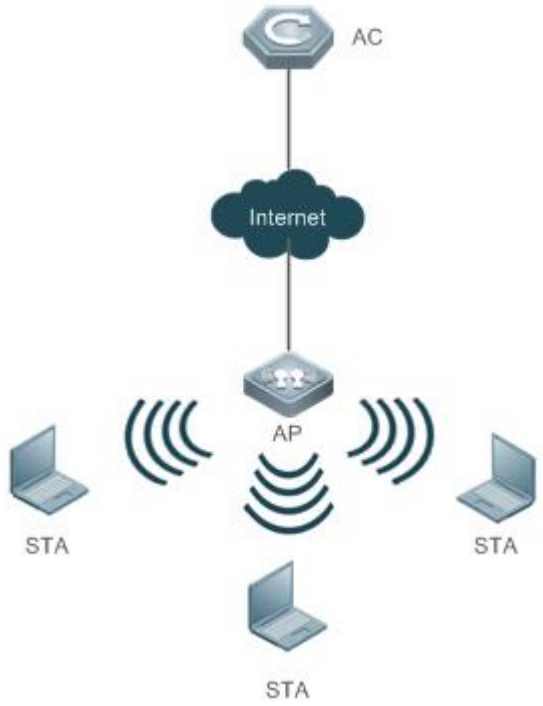
	| **tcp80 | tcp443** | **vrrp** } **pps** *value*
Parameter Description	**arp**: Specifies the ARP packet. **bpdu**: Specifies the IEEE BPDU packet. **capwap-disc**: Specifies the CAPWAP DISCOVER packet. **d1x**: Specifies the 802.1x EAPOL packet. **dhcp-option82**: Specifies the DHCP OPTION82 packet. **dhcp-relay-client**: Specifies the DHCP RELAY CLIENT packet. **dhcp-relay-server**: Specifies the DHCP RELAY SERVER packet. **dhcps**: Specifies the DHCP SNOOPING packet. **igmp**: Specifies the IGMP packet. **ipmc**: Specifies the IPv4 multicast packet. **ipv6-nans**: Specifies the IPv6 neighbor discovery packet. **isis**: Specifies the ISIS packet. **lldp**: Specifies the LLDP packet. **ospf**: Specifies the OSPF packet. **ospfv3**: Specifies the OSPF version3 packet. **pppoe**: Specifies the PPPOE packet. **pim**: Specifies the PIM packet. **rip**: Specifies the IPv4 RIP packet. **ripng**: Specifies the IPv6 RIP packet. **tcp80**: Specifies the Web authentication redirection packet. **Tcp443**: Specifies the HTTPS packet. **vrrp**: Specifies the VRRP packet. **pps** *value*: Specifies the upper limit of packets per second, ranging from 0 to 148,810pps.
Defaults	The default values vary with the product model.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show cpu-protect summary** command to display the configuration.

Configuration Example

Configuring Rate Limit for ARP Packets to 200pps

Scenario Figure 3-3	
Configuration Steps	● Configure the rate limit for ARP packets on the AC.
AC	Ruijie#configure terminal Ruijie(config)#cpu-protect type arp pps 200
Verification	After a user configures the rate limit for ARP packets on the AC, the system limits the rate for ARP packets arriving at the CPU based on the new rate limit. ● Run the **show cpu-protect summary** command to check the parameters set by the user. ● Run the **show cpu-protect type arp** command to display statistics about the received ARP packets.
AC	Ruijie#show cpu-protect summary Type Pps ------------------ --------- arp 1000 d1x 128 bpdu 128 lldp 128 dhcp-relay-server 128 dhcp-relay-client 128 dhcps 128 dhcp-option82 128 capwap-disc 128 ipv6-nans 128

```
rip                  128
pppoe                128
ripng                600
ospf                 600
ospfv3               600
isis                 128
vrrp                 128
igmp                 500
pim                  1000
ipmc                 128
tcp80                1200
tcp443               100
Ruijie#show cpu-protect type arp
Type                 Pps       Total     Drop
-------------------- --------- --------- ---------
arp                   1000      128089    0
```

Common Errors

N/A

3.4.2 Configuring the Rate Limit for Wireless Management Packets

Configuration Effect

- Configure the rate limit for wireless management packets.

Notes

N/A

Configuration Steps

↘ Configuring the Rate Limit for Wireless Management Packets

- Optional. This function is supported only on the AC. By default, the CTI-based rate limit is 8pps. Different ACs adopt different default AC-based rate limits.
- Enable the rate limiting function for wireless management packets on all ACs unless otherwise specified.
- Users can adjust the default rate limit based on CTI or the AC according to actual situations.

Command	**mgmt-ratelimit** { **disable** | **per-cti pps** *value* | **total pps** *value* }
Parameter Description	**disable**: Disables rate limiting function for wireless management packets. It is enabled by default. **per-cti pps** *value*: Configures the CTI-based rate limit, ranging from 1 to 10000pps. The default value is 8pps. **total pps** *value*: Configures the AC-based rate limit , ranging from 1 to 10000pps. Default values vary with

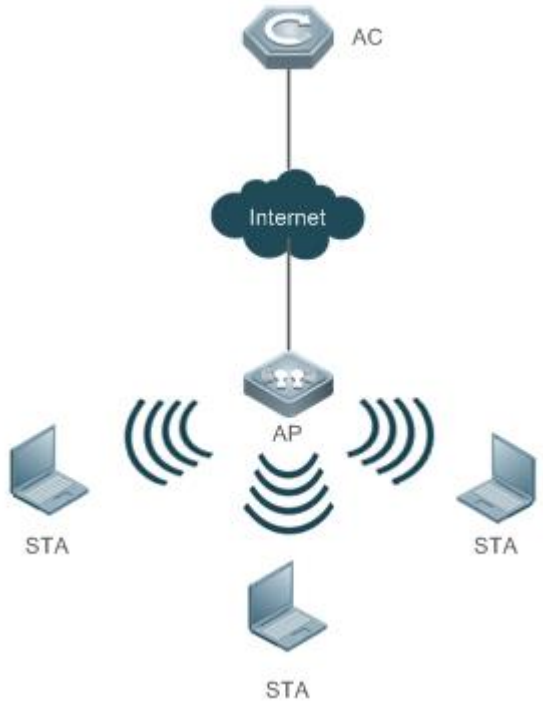
	different ACs.
Defaults	The rate limiting function is enabled by default. The default CTI-based rate limit is 8pps. The default AP-based rate limit varies with different ACs.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to display the rate limit of wireless management packets.

Configuration Example

Configuring the AC-based Rate Limit for Wireless Management Packets to 100pps

Scenario Figure 3-4	
Configuration Steps	● Configure the AC-based rate limit for wireless management packets.
AC	`Ruijie#configure terminal` `Ruijie(config)#mgmt-ratelimit total pps 200`
Verification	After a user configures the AC-based rate limit the system filters wireless management packets based on the new rate limit. ● Run the **show running-config** command to display the rate limit of wireless management packets.

	● Run the **show mgmt-ratelimit summary** command to display statistics about ARP packets.
AC	Ruijie#show running-config … mgmt-ratelimit total pps 200 … Ruijie#config terminal Ruijie(config)#sh mgmt-ratelimit summary pps max tpkts drop -------- -------- -------------------- -------------------- 0 40 1 0

Common Errors

N/A

3.5 Monitoring

Displaying

Description	Command
Displays the rate limit for packets of various types.	**show cpu-protect summary**
Displays statistics about specified packets.	**show cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** |**dhcp-realy-server** | **dhcps** | **igmp | ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3 | pim | pppoe** | **rip** | **ripng | tcp80** | **tcp443** | **vrrp** }
Displays the rate limit for wireless management packets.	**show running-config**
Displays statistics about CTI-based wireless management packets.	**show mgmt-ratelimit cti** *ifx*
Displays statistics about AP-based wireless management packets.	**show mgmt-ratelimit summary**

4 Configuring NFPP

4.1 Overview

The Network Foundation Protection Policy (NFPP) provides guard for switches.

Some malicious attacks are always found in the network environment. These attacks bring heavy burdens to switches, resulting in high CPU usage and abnormal running on switches. These attacks are as follows:

Denial of service (DoS) attacks may greatly consume the memory, entries, or other resources of a switch to cause system service unavailable.

Massive packet traffic is directed to the CPU, occupying the entire bandwidth of packets sent to the CPU. In this case, normal protocol traffic and management traffic cannot be processed by the CPU, causing protocol flapping or management failure. The forwarding on the data plane will also be affected and the entire network will become abnormal.

A great number of packets directed to the CPU consume massive CPU resources, making the CPU highly loaded and thereby causing device management failure or causing abnormal running.

NFPP can effectively protect the system from these attacks. Under attacks, NFPP protects proper running of various system services and keeps a low CPU load, thereby ensuring stable running of the entire network.

4.2 Applications

Application	Description
Attack Detection and Rate Limiting	Due to various malicious attacks such as ARP attacks and IP scanning attacks in the network, the CPU cannot process normal protocol and management traffic, causing protocol flapping or management failure. The NFPP attack detection and rate limiting function is used to limit the rate of attack traffic or isolate attack traffic so that the network can be recovered.
Centralized Rate Limiting and Distribution	Since normal service traffic is too large, you need to classify and prioritize the traffic. When a large number of packets are directed to the CPU, the CPU will be highly loaded, thereby causing device management or device running failure. The centralized rate limiting and distribution function is used to increase the priority of such traffic so that switches can run stably.

4.2.1 Attack Detection and Rate Limiting

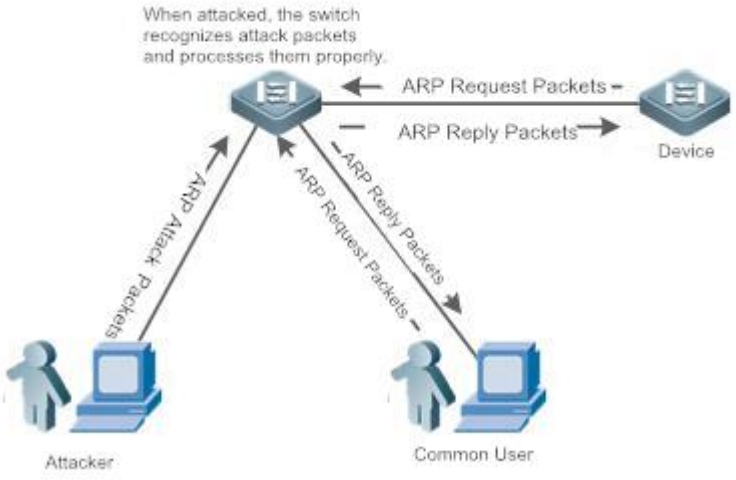
Scenario

NFPP supports attack detection and rate limiting for various types of packets, including Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Dynamic Host Configuration Protocol (DHCP) packets. It also allows users to define packet matching characteristics and corresponding attack detection and rate limiting policies. The attack detection and

rate limiting function takes effect based on each type of packets. This section uses ARP packets as an example to describe the scenario.

If an attacker sends ARP attack packets while the CPU capability is insufficient, a large number of CPU resources will be consumed for processing these ARP packets. If the attacker's ARP packet rate exceeds the maximum ARP bandwidth specified in the CPU Protect Policy (CPP) of the switch, packet loss occurs among normal ARP packets. As shown in Figure 4-1, common users will fail to access the network, and the switch will fail to send ARP responses to other devices.

Figure 4-1



Deployment

- By default, the ARP attack detection and rate limiting function is enabled, with corresponding policies configured. If an attacker's ARP packet rate exceeds the rate limit, the packets will be discarded. If the packet rate exceeds the attack threshold, a monitored host will be generated and prompt information will be output.
- If an attacker's ARP packet rate exceeds the rate limit defined in the CPP and affects normal ARP responses, you can enable attack isolation to discard ARP attack packets based on an ACL and recover the network.

For description of CPP configurations, refer to the "CPP" section.

To maximize the use of NFPP guard functions, modify the rate limits for various services in the CPP based on the application environment or use the configurations recommended by the system. You can run the **show cpu-protect summary** command to display the configurations.

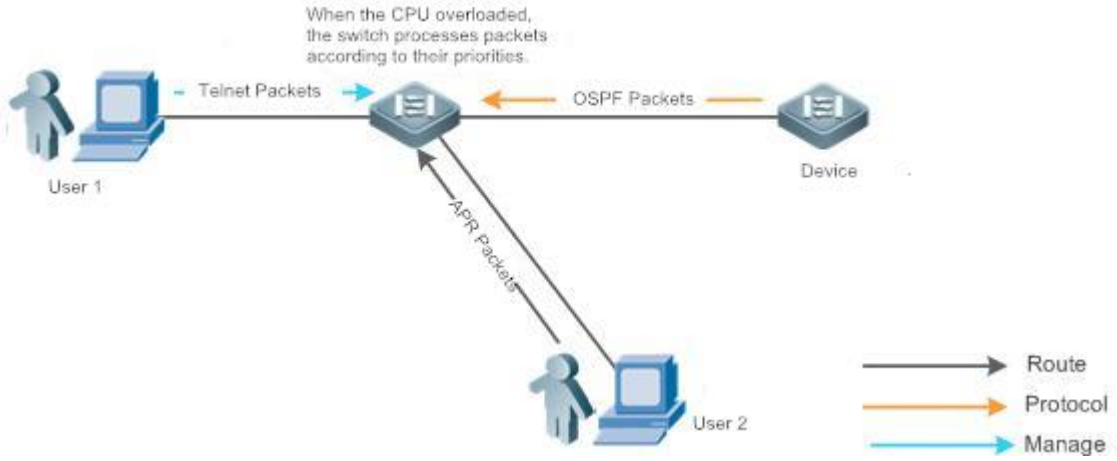
4.2.2 Centralized Rate Limiting and Distribution

Scenario

A switch classifies services defined in the CPP into three types: Manage, Route, and Protocol. Each type of services has an independent bandwidth. Different types of services cannot share their bandwidths. Traffic exceeding the bandwidth threshold is discarded. By such service classification, service packets of a certain type can be processed first.

As shown in Figure 4-2, the switch receives a large number of Telnet packets, OSPF packets, and ARP packets, causing CPU overload. In this case, the CPU cannot process all packets, and a large number of packets are backlogged in the queue, causing various problems such as occasional Telnet disconnection, OSPF protocol flapping, and ARP access failure to hosts.

Figure 4-2



Deployment

- By default, CPU centralized protection is enabled to assign an independent bandwidth and bandwidth ratio to each type of services. At the time, the CPU first processes Telnet packets to ensure uninterrupted connection of the Telnet service, and then processes OSPF packets to maintain OSPF protocol stability, and finally processes ARP packets.
- If the preceding problems occur in default configurations, you can accordingly adjust the bandwidth and bandwidth ratio for various types of services.

4.3 Features

Basic Concepts

↘ ARP Guard

In local area networks (LANs), IP addresses are converted to MAC addresses through ARP, which is significant for safeguarding network security. A large number of illegal ARP packets are sent to the gateway through the network, causing failure of the gateway to provide services for normal hosts. Such packets are called ARP-based DoS attacks. To prevent such attacks, limit the rate of ARP packets and detect and isolate the attack source.

↘ IP Anti-scanning

Many hacker attacks and network virus intrusions start from scanning active hosts in the network. Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failure.

To solve this problem, Layer-3 switches provide IP guard to prevent scanning by hackers and Blaster Worm viruses and reduce the CPU load. Currently, there are mainly two types of IP attacks:

- Scanning destination IP address changes: As the greatest threat to the network, this type of attacks not only consumes network bandwidth and increases device load but also is a prelude of most hacker attacks.
- Sending IP packets to non-existing destination IP addresses at high rates: This type of attacks is mainly designed for consuming the CPU load. For a Layer-3 device, if the destination IP address exists, packets are directly forwarded by the switching chip without occupying CPU resources. If the destination IP address does not exist, IP packets are sent to the CPU, which then sends ARP requests to query the MAC address corresponding to the destination IP address. If too many packets are sent to the CPU, CPU resources will be consumed. This type of attacks is less destructive than the former ones.

To prevent the latter type of attacks, limit the rate of IP packets and detect and isolate the attack source.

ICMP Guard

ICMP is a common approach for diagnosing network failures. After receiving an ICMP echo request from a host, the router or switch returns an ICMP echo reply. The preceding process requires the CPU to process the packets, thereby definitely consuming part of CPU resources. If an attacker sends a large number of ICMP echo requests to the destination device, massive CPU resources will be consumed on the device, and the device may even fail to work properly. This type of attacks is called ICMP flood. To prevent this type of attacks, limit the rate of ICMP packets and detect and isolate the attack source.

DHCP Guard

DHCP is widely used in LANs to dynamically assign IP addresses. It is significant for network security. Currently, the most common DHCP attacks, also called DHCP exhaustion attacks, use faked MAC addresses to broadcast DHCP requests. Various attack tools on the live network can easily complete this type of attacks. A network attacker can send sufficient DHCP requests to use up the address space provided by the DHCP server within a period. In this case, authorized hosts will fail to request DHCP IP addresses and thereby fail to access the network. To prevent this type of attacks, limit the rate of DHCP packets and detect and isolate the attack source.

DHCPv6 Guard

DHCP version 6 (DHCPv6) is widely used in LANs to dynamically assign IPv6 addresses. Both DHCP version 4 (DHCPv4) and DHCPv6 have security problems. Attacks to DHCPv4 also apply to DHCPv6. A network attacker can send a large number of DHCPv6 requests to use up the address space provided by the DHCPv6 server within a period. In this case, authorized hosts will fail to request IPv6 addresses and therefore fail to access the network. To prevent this type of attacks, limit the rate of DHCPv6 packets and detect and isolate the attack source.

ND Guard

Neighbor Discovery (ND) is mainly used in IPv6 networks to perform address resolution, router discovery, prefix discovery, and redirection. ND uses five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect. These packets are called ND packets.

ND snooping monitors ND packets in the network to filter unauthorized ND packets. It also monitors IPv6 hosts in the network and binds the monitored IPv6 hosts to ports to prevent IPv6 address stealing. ND snooping requires ND packets to

be sent to the CPU. If ND packets are sent at a very high rate, the CPU will be attacked. Therefore, ND guard must be provided to limit the rate of ND packets.

Overview

Feature	Description
Host-based Rate Limiting and Attack Identification	Limit the rate according to the host-based rate limit and identify host attacks in the network.
Port-based Rate Limiting and Attack Identification	Limit the rate according to the port-based rate limit and identify port attacks.
Configuring the Monitoring Period	Monitor host attackers in a specified period.
Configuring the Isolation Period	Isolate host attackers or port attackers in a specified period.
Configuring Trusted Hosts	Trust a host by not monitoring it.
Centralized Rate Limiting and Distribution	Classify and prioritize packets.

4.3.1 Host-based Rate Limiting and Attack Identification

Limit the rate of attack packets of hosts and identify the attacks.

Identify ARP scanning.

Identify IP scanning.

Working Principle

Hosts can be identified in two ways: based on the source IP address, VLAN ID, and port and based on the link-layer source MAC address, VLAN ID, and port. Each host has a rate limit and an attack threshold (also called alarm threshold). The rate limit must be lower than the attack threshold. If the attack packet rate exceeds the rate limit of a host, the host discards the packets beyond the rate limit. If the attack packet rate exceeds the attack threshold of a host, the host identifies host attacks, records them in logs, and sends Trap packets.

ARP scanning attacks may have occurred if ARP packets beyond the scanning threshold received in the configured period meet either of the following conditions:

- The link-layer source MAC address is fixed but the source IP address changes.
- The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes.

Among IP packets beyond the scanning threshold received in the configured period, if the source IP address remains the same while the destination IP address continuously changes, IP scanning attack may have occurred.

When NFPP detects a specific type of attack packets under a service, it sends an alarm to the administrator. If the attack traffic persists, NFPP will not resend the alarm within 60 seconds after generating an alarm.

To prevent CPU resource consumption caused by frequent log printing, NFPP writes attack detection logs to the buffer, obtains them from the buffer at a specified rate, and prints them. NFPP does not limit the rate of Trap packets.

At present, only ARP guard and IP anti-scanning support anti-scanning.

4.3.2 Port-based Rate Limiting and Attack Identification

Limit the rate of port-based attack packets and identify the attacks.

Working Principle

Each port has a rate limit and an attack threshold. The rate limit must be lower than the attack threshold. If the packet rate exceeds the rate limit on a port, the port discards the packets. If the packet rate exceeds the attack threshold on a port, the port records the attacks in logs and sends Trap packets.

4.3.3 Configuring the Monitoring Period

Configures the monitoring period for an attacker.

Working Principle

Monitored hosts provide information about attackers in the current system. If the isolation period is 0 (that is, no isolation), the guard module automatically performs software monitoring on attackers in the configured monitoring period. Within the monitoring period, you can view the entries of a monitored host. If attacks are received from this host before aging of the monitoring period, refresh the monitoring period of the host; otherwise, when the monitoring period is aged to 0, the entries of the monitored host will be deleted. When the isolation time is configured to a non-0 value, the guard module automatically isolates the host monitored by the software.

4.3.4 Configuring the Isolation Period

Configure the isolation period for an attacker.

Working Principle

Isolation is performed by the guard policy after attacks are detected. Isolation is implemented using the filtering function of a software ACL to ensure that these attacks are not sent to the CPU, thereby ensuring proper running of the device.

The isolation function supports host-based and port-based isolation. When an attacker is isolated, a policy will be configured into an ACL. When the ACL resources are exhausted and isolation fails, logs will be printed to remind the administrator.

4.3.5 Configuring Trusted Hosts

Configure trusted hosts.

Working Principle

If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host will be allowed to send packets of specified types to the CPU.

4.3.6 Centralized Rate Limiting and Distribution

Set the rate thresholds and percentages for Manage, Route and Protocol packets.

Working Principle

Services defined in the CPP are classified into three types: Manage, Route, and Protocol. (For details, see the following table.) Each type of services has an independent bandwidth. Different types of services cannot share their bandwidths. Traffic exceeding the bandwidth threshold is discarded. By such service classification, service packets of a certain type can be processed first.

NFPP allows the administrator to flexibly assign bandwidth for three types of packets based on the actual network environment so that Protocol and Manage packets can be first processed. Prior processing of Protocol packets ensures proper running of the protocol, and prior processing of Manage packets helps the administrator perform proper management, thereby ensuring proper running of important device functions and improving the guard capability of the device.

After rate limiting for the preceding packet types, all types of packets are centralized in a queue. When one type of service features a lower processing efficiency, packets of this service will be backlogged in the queue and may finally use up resources of the queue. NFPP allows the administrator to configure the percentages of these three types of packets in the queue. When the queue length occupied by one type of packets exceeds the product of the total queue length and the percentage of this type of packets, these packets are discarded. This effectively prevents one type of packets from exclusively occupying queue resources.

Packet Type	Service Type Defined in the CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, isis dhcps, gvrp, ripng, dvmrp, igmp, mpls, ospf, pim, pimv6, rip, vrrp, ospf3, dhcp-relay-s, dhcp-relay-c, option82, tunnel-bpdu, and tunnel-gvrp
Route	unknown-ipmc, unknown-ipmcv6, ttl1, ttl0, udp-helper, ip4-packet-other, ip6-packet-other, and non-ip-packet-other
Manage	ip4-packet-local, ip6-packet-local, and arp

For the definitions of service types, see the *CPP Configuration Guide*.

4.4 Configuration

Configuration	Description and Command	
Configuring ARP Guard	(Mandatory) It is used to configure the global ARP guard function.	
	arp-guard enable	Enables global attack detection.
	arp-guard monitor-period	Configures the monitoring period.
	arp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	arp-guard rate-limit	Configures the global rate limit.
	arp-guard attack-threshold	Configures the global attack threshold.
	arp-guard scan-threshold	Configures the global host-based scanning threshold.

Configuration	Description and Command	
	(Optional) It is used to configure ARP isolation and ARP guard.	
	arp-guard isolate-period	Configures the global isolation period.
	arp-guard trusted-host	Configures trusted hosts.
	nfpp arp-guard enable	Enables attack detection for a port.
	nfpp arp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp arp-guard scan-threshold	Configures the stage-by-stage scanning threshold for a port.
	nfpp arp-guard isolate-period	Configures the isolation period for a port.
Configuring IP Anti-scanning	(Mandatory) It is used to configure the global IP anti-scanning function.	
	ip-guard enable	Enables global attack detection.
	ip-guard monitor-period	Configures the monitoring period.
	ip-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	ip-guard rate-limit	Configures the global rate limit.
	ip-guard attack-threshold	Configures the global attack threshold.
	ip-guard scan-threshold	Configures the global host-based scanning threshold.
	(Optional) It is used to configure IP trusted hosts, IP isolation and port-based IP anti-scanning.	
	ip-guard isolate-period	Configures the global isolation period.
	ip-guard trusted-host	Configures trusted hosts.
	nfpp ip-guard enable	Enables attack detection for a port.
	nfpp ip-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp ip-guard scan-threshold	Configures the stage-by-stage scanning threshold for a port.
	nfpp ip-guard isolate-period	Configures the isolation period for a port.
Configuring ICMP Guard	(Mandatory) It is used to configure the global ICMP guard function.	
	icmp-guard enable	Enables global attack detection.
	icmp-guard monitor-period	Configures the monitoring period.
	icmp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	icmp-guard rate-limit	Configures the global rate limit.
	icmp-guard attack-threshold	Configures the global attack threshold.

Configuration	Description and Command	
	(Optional) It is used to configure ICMP trusted hosts, ICMP isolation and port-based ICMP guard.	
	icmp-guard isolate-period	Configures the global isolation period.
	icmp-guard trusted-host	Configures trusted hosts.
	nfpp icmp-guard enable	Enables attack detection for a port.
	nfpp icmp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp icmp-guard isolate-period	Configures the isolation period for a port.
Configuring DHCP Guard	(Mandatory) It is used to configure the global DHCP guard function.	
	dhcp-guard enable	Enables global attack detection.
	dhcp-guard monitor-period	Configures the monitoring period.
	dhcp-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	dhcp-guard rate-limit	Configures the global rate limit.
	dhcp-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure DHCP isolation and port-based DHCP guard.	
	dhcp-guard isolate-period	Configures the global isolation period.
	dhcp-guard trusted-host	Configures trusted hosts.
	nfpp dhcp-guard enable	Enables attack detection for a port.
	nfpp dhcp-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp dhcp-guard isolate-period	Configures the isolation period for a port.
Configuring DHCPv6 Guard	(Mandatory) It is used to configure the global DHCPv6 guard function.	
	dhcpv6-guard enable	Enables global attack detection.
	dhcpv6-guard monitor-period	Configures the monitoring period.
	dhcpv6-guard monitored-host-limit	Configures the maximum number of monitored hosts.
	dhcpv6-guard rate-limit	Configures the global rate limit.
	dhcpv6-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure DHCPv6 isolation and DHCPv6 guard.	
	dhcpv6-guard isolate-period	Configures the global isolation period.
	dhcpv6-guard trusted-host	Configures trusted hosts.
	nfpp dhcpv6-guard enable	Enables attack detection for a port.
	nfpp dhcpv6-guard policy	Configures the rate limit and attack threshold for a port.
	nfpp dhcpv6-guard isolate-period	Configures the isolation period for a port.

Configuration	Description and Command	
Configuring ND Guard	(Mandatory) It is used to configure the global ND guard function.	
	nd-guard enable	Enables global attack detection.
	nd-guard rate-limit	Configures the global rate limit.
	nd-guard attack-threshold	Configures the global attack threshold.
	(Optional) It is used to configure the port-based ND guard function.	
	nd-guard trusted-host	Configures trusted hosts.
	nfpp nd-guard enable	Enables attack detection for a port.
	nfpp nd-guard policy	Configures the rate limit and attack threshold for a port.
Configuring Centralized Rate Limiting and Distribution	(Optional) It is used to set the rate thresholds and percentages for Manage, Route and Protocol packets.	
	cpu-protect sub-interface pps	Configures the maximum bandwidth for each type of packets.
	cpu-protect sub-interface percent	Configures the maximum percentage of each type of packets in the queue.
Configuring NFPP Log Information	(Mandatory) It is used to set log information.	
	log-buffer entries	Configures the capacity of NFPP log buffer.
	log-buffer logs	Configures the rate when logs are obtained from the log buffer to generate system messages.
	(Optional) It is used to set logs to be recorded.	
	logging vlan	Specifies the VLANs in which logs need to be recorded.
	logging interface	Specifies the port on which logs need to be recorded.

4.4.1 Configuring ARP Guard

Configuration Effect

- ARP attacks are identified based on hosts or ports. Host-based ARP attack identification supports two modes: identification based on the source IP address, VLAN ID, and port and identification based on the link-layer source MAC address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the ARP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ARP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

- ARP guard can also detect ARP scanning attacks. ARP scanning attacks indicate that the link-layer source MAC address is fixed but the source IP address changes, or that the link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes. Due to the possibility of misjudgment, hosts possibly performing ARP scanning are not isolated and are provided for the administrator's reference only.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.
- ARP guard prevents only ARP DoS attacks to the switch, but not ARP spoofing or ARP attacks in the network.

Configuration Steps

Enabling Attack Detection

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If ARP guard is disabled, the system automatically clears monitored hosts, scanned hosts, and port isolation entries.

Command	**arp-guard enable**
Parameter Description	-
Defaults	ARP guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp arp-guard enable**
Parameter Description	-
Defaults	ARP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ARP guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AC device.

- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AC device.

Command	**arp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	-

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Configure the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AC device.

- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**arp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Configuring the Attack Threshold

- Mandatory.
- To achieve the best ARP guard effect, you are advised to configure the host-based rate limit and alarm threshold based on the following rules: Source IP address-based rate limit < Source IP address-based alarm threshold < Source MAC address-based rate limit < Source MAC address-based alarm threshold.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over source IP address-based rate limiting while the latter takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **arp-guard rate-limit** {**per-src-ip** | **per-src-mac**} *pps* command to configure rate limits of hosts identified based on the source IP address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port.
- In NFPP configuration mode: run the **arp-guard attack-threshold** {**per-src-ip** | **per-src-mac**} *pps* command to configure attack thresholds of hosts identified based on the source IP address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port.
- In interface configuration mode: run the **nfpp arp-guard policy** {**per-src-ip | per-src-mac**} *rate-limit-pps attack-threshold-pps* command to configure rate limits and attack thresholds of hosts identified based on the source IP

address, VLAN ID, and port and of hosts identified based on the link-layer source MAC address, VLAN ID, and port on an interface.

Command	**arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-src-mac:** Limits the rate of packets from each source MAC address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	the default rate limit varies with the product model.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**arp-guard attack-threshold** { **per-src-ip** | **per-src-mac | per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is packets per second (pps).
Defaults	the default attack thresholds vary with the product model.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp arp-guard policy** { **per-src-ip | per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the rate limit and attack threshold for each source IP address. **per-src-mac:** Configures the rate limit and attack threshold for each source MAC address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Scanning Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- The ARP scanning table stores only the latest 256 records. When the ARP scanning table is full, the latest record will overwrite the earliest record.

- ARP scanning attack may have occurred if ARP packets received within 10 seconds meet either of the following conditions:
  - The link-layer source MAC address is fixed but the source IP address changes.
  - The link-layer source MAC address and source IP address are fixed but the destination IP address continuously changes, and the change times exceed the scanning threshold.

Command	**arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	The default scanning threshold is 100 in the unit of 10 seconds.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	By default, no port-based ARP scanning threshold is configured and the global ARP scanning threshold is used.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ARP guard, you can configure only a maximum of 500 IP addresses and MAC addresses not to be monitored.
- Support the global configuration mode on the AC device.
- If any entry matching a trusted host (the IP addresses and MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.1 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.1 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.1 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.1 0000.0000.1111 is not found." to notify the administrator.

Command	**arp-guard trusted-host** *ip mac*
Parameter Description	*ip*: Indicates the IP address. *mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send ARP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends ARP attack packets to a switch configured with ARP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on ARP Guard

Scenario	● ARP host attacks exist in the system, and some hosts fail to properly establish an ARP connection. ● ARP scanning exists in the system, causing a very high CPU usage. ● ARP packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Set the host-based attack threshold to 5 pps. ● Set the ARP scanning threshold to 10 pps. ● Set the isolation period to 180 pps. ● Configure trusted hosts.
	`Ruijie# configure terminal` `Ruijie(config)# nfpp` `Ruijie (config-nfpp)#arp-guard rate-limit per-src-mac 5` `Ruijie (config-nfpp)#arp-guard attack-threshold per-src-mac 10` `Ruijie (config-nfpp)#arp-guard isolate-period 180` `Ruijie (config-nfpp)#arp-guard trusted-host 1.1.1.1 0000.0000.1111`
Verification	● Run the **show nfpp arp-guard summary** command to display the configurations.
	`(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)` `Interface Status  Isolate-period Rate-limit  Attack-threshold Scan-threshold`

	Global Disable 180 4/5/100 8/10/200 15 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp arp-guard hosts** command to display monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address MAC address remain-time(s) ---- --------- ---------- ---------- -------------- 1 Gi0/43 5.5.5.16 - 175 Total: 1 host
	● Run the **show nfpp arp-guard scan** command to display scanned hosts.
	VLAN interface IP address MAC address timestamp ---- --------- ---------- ---------- --------- 1 Gi0/5 - 001a.a9c2.4609 2013-4-30 23:50:32 1 Gi0/5 192.168.206.2 001a.a9c2.4609 2013-4-30 23:50:33 1 Gi0/5 - 001a.a9c2.4609 2013-4-30 23:51:33 1 Gi0/5 192.168.206.2 001a.a9c2.4609 2013-4-30 23:51:34 Total: 4 record(s)
	● Run the **show nfpp arp-guard trusted-host** command to display trusted hosts.
	IP address mac ---------- ---- 1.1.1.1 0000.0000.1111 Total: 1 record(s)

4.4.2 Configuring IP Anti-scanning

Configuration Effect

- IP attacks are identified based on hosts or ports. In host-based IP attack identification, IP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the IP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the IP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

- IP guard can also detect IP scanning attacks. IP anti-scanning applies to IP packet attacks as follows: the destination IP address continuously changes but the source IP address remains the same, and the destination IP address is not the IP address of the local device.
- IP anti-scanning applies to IP packet attacks where the destination IP address is not the local IP address. The CPP limits the rate of IP packets where the destination IP address is the local IP address.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AC device.
- If IP anti-scanning is disabled, the system automatically clears monitored hosts.

Command	**ip-guard enable**
Parameter Description	-
Defaults	IP anti-scanning is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp ip-guard enable**
Parameter Description	-
Defaults	IP anti-scanning is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	IP anti-scanning configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AC device.

- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. **permanent**: Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AC device.

Command	**ip-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.

- Support the global configuration mode on the AC device.
- If the number of monitored hosts reaches 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**ip-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **ip-guard rate-limit** { **per-src-ip** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp ip-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**ip-guard rate-limit** { **per-src-ip**	**per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.

Defaults	**per-src-ip**: 20 pps. **per-port**: 1,500 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	**per-src-ip**: 20 pps. **per-port**: 1,500 pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp ip-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring the Scanning Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- IP scanning attack may have occurred if IP packets received within 10 seconds meet the following conditions:
  - The source IP address remains the same.
  - The destination IP address continuously changes and is not the local IP address, and the change times exceed the scanning threshold.

Command	**ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	The default scanning threshold is 100 pps.

Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold, ranging from 1 to 9,999.
Defaults	By default, no port-based IP scanning threshold is configured and the global IP scanning threshold is used.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For IP anti-scanning, you can configure a maximum of 500 IP addresses not to be monitored.
- Support the global configuration mode on the AC device.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.

Command	**ip-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send IP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends IP attack packets to a switch configured with IP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on IP Guard

Scenario	● IP host attacks exist in the system, and packets of some hosts cannot be properly routed and forwarded. ● IP scanning exists in the system, causing a very high CPU usage. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Configure the IP scanning threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.
	`Ruijie# configure terminal` `Ruijie(config)# nfpp` `Ruijie (config-nfpp)#ip-guard rate-limit per-src-ip 20` `Ruijie (config-nfpp)#ip-guard attack-threshold per-src-ip 30` `Ruijie (config-nfpp)#ip-guard isolate-period 180` `Ruijie (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255`
Verification	● Run the **show nfpp ip-guard summary** command to display the configurations.
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) `Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold` `Global Disable 180 20/-/100 30/-/200 100` Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the show nfpp ip-guard hosts command to display monitored hosts.
	`If col_filter 1 shows '*', it means "hardware do not isolate host".` `VLAN interface IP address Reason remain-time(s)`

	`` ---- --------- ---------- ------ -------------- 1 Gi0/5 192.168.201.47 ATTACK 160 Total: 1 host ```
	● Run the **show nfpp ip-guard trusted-host** command to display trusted hosts.
	`` IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s) ```

4.4.3 Configuring ICMP Guard

Configuration Effect

- ICMP attacks are identified based on hosts or ports. In host-based attack identification, ICMP attacks are identified based on the source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the ICMP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ICMP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AC device.
- If ICMP guard is disabled, the system automatically clears monitored hosts.

Command	**icmp-guard enable**
Parameter Description	-
Defaults	ICMP guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp icmp-guard enable**
Parameter Description	-
Defaults	ICMP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ICMP guard configured in interface configuration mode takes priority over that in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.

- Support the global configuration mode on the AC device.

Command	**icmp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AC device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**icmp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp icmp-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Limits the rate for each source IP address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AC devices, see the specification and limitation document. For the AP device: **per-src-ip**: 200 pps; **per-port**: 400 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
Parameter Description	**per-src-ip:** Configures the attack threshold for each source IP address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AC devices, see the specification and limitation document. For the AP device: **per-src-ip**: 200 pps; **per-port**: 400 pps.

Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp icmp-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-ip:** Configures the rate limit and attack threshold for each source IP address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ICMP anti-scanning, you can configure a maximum of 500 IP addresses not to be monitored.
- Support the global configuration mode on the AC device.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 1.1.1.0 255.255.255.0 is not found." to notify the administrator.

Command	**icmp-guard trusted-host** *ip mask*
Parameter Description	*ip*: Indicates the IP address. *mask*: Indicates the mask of an IP address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode

Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send ICMP packets to the CPU, without any rate limiting or alarm reporting. You can configure the mask so that no host in one network segment is monitored. You can configure a maximum of 500 trusted hosts.

Verification

When a network host sends ICMP attack packets to a switch configured with ICMP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

↘ CPU Protection Based on ICMP Guard

Scenario	● ICMP host attacks exist in the system, and some hosts cannot successfully ping devices. ● Packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.
	`Ruijie# configure terminal` `Ruijie(config)# nfpp` `Ruijie (config-nfpp)#icmp-guard rate-limit per-src-ip 20` `Ruijie (config-nfpp)#icmp-guard attack-threshold per-src-ip 30` `Ruijie (config-nfpp)#icmp-guard isolate-period 180` `Ruijie (config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255`
Verification	● Run the **show nfpp icmp-guard summary** command to display the configurations.
	`(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)` `Interface Status  Isolate-period Rate-limit  Attack-threshold` `Global  Disable 180  20/-/400  30/-/400` `Maximum count of monitored hosts: 1000` `Monitor period: 600s`
	● Run the **show nfpp icmp-guard hosts** command to display monitored hosts.

	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface IP address remain-time(s) ---- --------- ---------- -------------- 1 Gi0/5 192.168.201.47 160 Total: 1 host
	• Run the **show nfpp icmp-guard trusted-host** command to display trusted hosts.
	IP address mask ---------- ---- 192.168.201.46 255.255.255.255 Total: 1 record(s)

4.4.4 Configuring DHCP Guard

Configuration Effect

- DHCP attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the DHCP packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCP packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets. In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AC device.
- If DHCP guard is disabled, the system automatically clears monitored hosts.

Command	**dhcp-guard enable**
Parameter Description	-
Defaults	Attack detection is enabled by default.
Command Mode	NFPP configuration mode

Usage Guide	-

Command	**nfpp dhcp-guard enable**
Parameter Description	-
Defaults	DHCP guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCP guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AC device.

Command	**dhcp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AC device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**dhcp-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored

	hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**dhcp-guard rate-limit** { **per-src-mac**	**per-port** } *pps*
Parameter Description	**per-src-mac:** Limits the rate for each source MAC address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AC devices, the default rate limit varies with the product model. For the AP devices, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on port is 150 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**dhcp-guard attack-threshold** { **per-src-mac**	**per-port** } *pps*
Parameter Description	**per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port.

	pps: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AC devices, the default rate limit varies with the product model. For the AP devices, the default rate limit for packets based on source MAC address is 10 pps, and the default rate limit for packets based on port is 300 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-mac:** Configures the rate limit and attack threshold for each source MAC address**.** **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For DHCP guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AC device.
- If any entry matching a trusted host (MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**dhcp-guard trusted-host** *mac*
Parameter	*mac*: Indicates the MAC address.

Description	
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send DHCP packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends DHCP attack packets to a switch configured with DHCP attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

CPU Protection Based on DHCP Guard

Scenario	DHCP host attacks exist in the system, and some hosts fail to request IP addresses. DHCP packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.
	`Ruijie# configure terminal` `Ruijie(config)# nfpp` `Ruijie (config-nfpp)#dhcp-guard rate-limit per-src-mac 8` `Ruijie (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16` `Ruijie (config-nfpp)#dhcp-guard isolate-period 180` `Ruijie (config-nfpp)#dhcp-guard trusted-host 0000.0000.1111`
Verification	● Run the **show nfpp dhcp-guard summary** command to display the configurations.
	`(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)` `Interface Status  Isolate-period Rate-limit  Attack-threshold` `Global  Disable 180  -/8/150  -/16/300` `Maximum count of monitored hosts: 1000`

	Monitor period: 600s
	• Run the **show nfpp dhcp-guard hosts** command to display monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host
	• Run the **show nfpp dhcp-guard trusted-host** command to display trusted hosts.
	mac ---- 0000.0000.1111 Total: 1 record(s)

4.4.5 Configuring DHCPv6 Guard

Configuration Effect

- DHCPv6 attacks are identified based on hosts or ports. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and port. Each type of attack identification has a rate limit and an alarm threshold. If the DHCPv6 packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the DHCPv6 packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets.
- In host-based attack identification, the system also isolates the attack source.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AC device.
- If DHCPv6 guard is disabled, the system automatically clears monitored hosts.

Command	**dhcpv6-guard enable**
Parameter	-

Description	
Defaults	Attack detection is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp dhcpv6-guard enable**
Parameter Description	-
Defaults	DHCPv6 guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet traffic of attackers exceeds the rate limit of the CPP, you can configure the isolation period to directly discard packets and therefore save bandwidth resources.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Command	**dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	NFPP configuration mode
Usage Guide	The attacker isolation period falls into two types: global isolation period and port-based isolation period (local isolation period). For a port, if the port-based isolation period is not configured, the global isolation period is used; otherwise, the port-based isolation period is used.

Command	**nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period in the unit of second. It can be set to 0 or any value from 30 to 86,400. The value 0 indicates no isolation. **permanent:** Indicates permanent isolation.
Defaults	By default, a global isolation period is used, but no local isolation period is configured.

Command Mode	Interface configuration mode
Usage Guide	-

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is directly used as the attacker monitoring period, and the configured monitoring period does not take effect.
- Support the global configuration mode on the AC device.

Command	**dhcpv6-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period in the unit of second. The value ranges from 180 to 86,400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is 0, the system performs software monitoring on detected attackers. The timeout period is the monitoring period. During software monitoring, if the isolation period is set to a non-zero value, the system automatically performs isolation against attackers monitored by software and sets the timeout period as the monitoring period. The monitoring period is valid only when the isolation period is 0. If the isolation period is changed to 0, attackers under the corresponding port is deleted, instead of being monitored by software.

Configuring the Maximum Number of Monitored Hosts

- Mandatory.
- Increase the maximum number of monitored hosts. As the number of actually monitored hosts increases, more CPU resources are used to handle monitored hosts.
- Support the global configuration mode on the AC device.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Command	**dhcpv6-guard monitored-host-limit** *number*
Parameter Description	*number*: Indicates the maximum number of monitored hosts, ranging from 1 to 4,294,967,295.
Defaults	The maximum number of monitored hosts is 1000 by default.

Command Mode	NFPP configuration mode
Usage Guide	If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to a value smaller than 1000. In this case, the system does not delete monitored hosts but prints the information "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." This information notifies the administrator that the configuration does not take effect and that part of monitored hosts need to be deleted. If the table of monitored hosts is full, the system prints the log "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." to notify the administrator.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes priority over port-based rate limiting.
- In NFPP configuration mode: run the **dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** } *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp dhcpv6-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**dhcpv6-guard rate-limit** { **per-src-mac**	**per-port** } *pps*
Parameter Description	**per-src-mac:** Limits the rate for each source MAC address. **per-port:** Limits the rate for each port. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AC devices, the default rate limit varies with the product model. For the AP devices, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on port is 150 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*
Parameter Description	**per-src-mac:** Configures the attack threshold for each source MAC address. **per-port:** Configures the attack threshold for each port. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AC devices, the default rate limit varies with the product model. For the AP devices, the default rate limit for packets based on source MAC address is 10 pps, and the default rate limit for packets based on port is 300 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*
Parameter Description	**per-src-mac:** Configures the rate limit and attack threshold for each source MAC address. **per-port:** Configures the rate limit and attack threshold for each port. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For DHCPv6 guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AC device.
- If any entry matching a trusted host (MAC addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.

- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**dhcpv6-guard trusted-host** *mac*
Parameter Description	*mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send DCHPv6 packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends DHCPv6 attack packets to a switch configured with DHCPv6 attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold or scanning threshold, attack prompt information is displayed.
- If an isolation entry needs to be created for the attacker, attacker isolation prompt information is displayed.

Configuration Example

CPU Protection Based on DHCPv6 Guard

Scenario	DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts. DHCPv6 packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.
	`Ruijie# configure terminal` `Ruijie(config)# nfpp` `Ruijie (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8` `Ruijie (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16` `Ruijie (config-nfpp)#dhcpv6-guard isolate-period 180` `Ruijie (config-nfpp)#dhcpv6-guard trusted-host 0000.0000.1111`
Verification	● Run the **show nfpp dhcpv6-guard summary** command to display the configurations.
	`(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)` `Interface Status  Isolate-period Rate-limit  Attack-threshold`

	Global Disable 180 -/8/150 -/16/300 Maximum count of monitored hosts: 1000 Monitor period: 600s
	● Run the **show nfpp dhcpv6-guard hosts** command to display monitored hosts.
	If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ---- --------- ----------- -------------- *1 Gi0/5 001a.a9c2.4609 160 Total: 1 host
	● Run the **show nfpp dhcpv6-guard trusted-host** command to display trusted hosts.
	mac ---- 0000.0000.1111 Total: 1 record(s)

4.4.6 Configuring ND Guard

Configuration Effect

- AR ND guard classifies ND packets into three types based on their purposes: 1. NS and NA; 2. RS; 3. RA and Redirect. The first type of packets are used for address resolution. The second type of packets are used by hosts to discover the gateway. The third type of packets are related to routing: RAs are used to advertise the gateway and prefix while Redirect packets are used to advertise a better next hop.
- At present, only port-based ND packet attack identification is supported. You can configure the rate limits and alarm thresholds for these three types of packets. If the ND packet rate exceeds the rate limit, the packets beyond the rate limit are discarded. If the ND packet rate exceeds the alarm threshold, the system prints alarm information and sends Trap packets.

Notes

- For a command that is configured both in global configuration mode and interface configuration mode, the configuration in interface configuration mode takes priority over that configured in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Steps

↘ **Enabling Attack Detection**

- (Mandatory) Attack detection is enabled by default.
- Support the global configuration mode or interface configuration mode on the AC device.

Command	**nd-guard enable**
Parameter Description	-
Defaults	ND guard is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp nd-guard enable**
Parameter Description	-
Defaults	ND guard is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ND guard configured in interface configuration mode takes priority over that configured in global configuration mode.

Configuring the Attack Threshold

- Mandatory.
- Support the global configuration mode or interface configuration mode on the AC device.
- If the configured rate limit is greater than the attack threshold, the system prints the log "%ERROR: rate limit is higher than attack threshold 500pps." to notify the administrator.
- If the configured attack threshold is smaller than the rate limit, the system prints the log "%ERROR: attack threshold is smaller than rate limit 300pps." to notify the administrator.
- If the memory cannot be allocated to detected attackers, the system prints the log "%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- In NFPP configuration mode: run the **nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* command to configure the global rate limit.
- In NFPP configuration mode: run the **nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* command to configure the global attack threshold. That is, when the packet rate exceeds the attack threshold, it is considered that attack behaviors exist.
- In interface configuration mode: run the **nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps* command to configure the local rate limit and attack threshold on a port.

Command	**nd-guard rate-limit per-port** [**ns-na**	**rs**	**ra-redirect**] *pps*
Parameter	**ns-na:** Indicates NSs and NAs.

Description	**rs:** Indicates RSs. **ra-redirect:** Indicates RAs and Redirect packets. *pps*: Indicates the rate limit, ranging from 1 to 9,999.
Defaults	For the AC devices, the default attack threshold varies with the product model. For the AP devices, the default attack threshold for ns-na, rs, and ra-redirect packets is 15 pps.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*
Parameter Description	**ns-na:** Indicates NSs and NAs. **rs:** Indicates RSs. **ra-redirect:** Indicates RAs and Redirect packets. *pps*: Indicates the attack threshold, ranging from 1 to 9,999. The unit is pps.
Defaults	For the AC devices, the default attack threshold varies with the product model. For the AP devices, the default attack threshold for ns-na, rs, and ra-redirect packets is 30 pps.
Command Mode	NFPP configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit.

Command	**nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*
Parameter Description	**ns-na:** Indicates NSs and NAs. **rs:** Indicates RSs. **ra-redirect:** Indicates RAs and Redirect packets. *rate-limit-pps*: Indicates the rate limit, ranging from 1 to 9,999. *attack-threshold-pps*: Indicates the attack threshold, ranging from 1 to 9,999.
Defaults	By default, no rate limit and attack threshed are configured for a port, and the global rate limit and attack threshold are used.
Command Mode	Interface configuration mode
Usage Guide	The attack threshold must be equal to or greater than the rate limit. ND snooping classifies ports into two types: untrusted ports (connecting the host) and trusted ports (connecting to the gateway). As traffic on a trusted port is usually larger than that on an untrusted port, the rate limit for a trusted port is higher than that for an untrusted port. If ND snooping is enabled for a trusted port, ND snooping sets the rate limit to 800 pps and the attack threshold to 900 pps for the three types of packets on the port by advertising ND guard. ND guard treats the rate limit configured for ND snooping and that configured by the administrator in the same way. The value configured later overwrites the value configured earlier and is stored in the configuration file. The attack threshold configured for ND snooping is treated in a similar way.

Configuring Trusted Hosts

- (Optional) No trusted host is configured by default.
- For ND guard, you can configure a maximum of 500 MAC addresses not to be monitored.
- Support the global configuration mode on the AC or AP device.
- If the table of trusted hosts is full, the system prints the log "%ERROR: Attempt to exceed limit of 500 trusted hosts." to notify the administrator.
- If the administrator fails to delete a trusted host, the system prints the log "%ERROR: Failed to delete trusted host 0000.0000.1111." to notify the administrator.
- If you fail to add a trusted host, the system prints the log "%ERROR: Failed to add trusted host 0000.0000.1111." to notify the administrator.
- If the trusted host you want to add already exists, the system prints the log "%ERROR: Trusted host 0000.0000.1111 has already been configured." to notify the administrator.
- If the trusted host you want to delete does not exist, the system prints the log "%ERROR: Trusted host 0000.0000.1111 is not found." to notify the administrator.

Command	**nd-guard trusted-host** *mac*
Parameter Description	*mac*: Indicates the MAC address.
Defaults	No trusted host is configured by default.
Command Mode	NFPP configuration mode
Usage Guide	If you do not want to monitor a host, you can run the following commands to configure the host to be trusted. This trusted host can send ND packets to the CPU, without any rate limiting or alarm reporting.

Verification

When a network host sends ND attack packets to a switch configured with ND attack detection and rate limiting, check whether these packets can be sent to the CPU.

- If the rate of packets not meeting trusted host configuration exceeds the attack threshold for a port, attack prompt information is displayed.
- If the rate of attack packets meets the trusted host configuration, no prompt information is displayed.

Configuration Example

CPU Protection Based on ND Guard

Scenario	ND host attacks exist in the system, and neighbor discovery fails on some hosts. ND packet traffic of some hosts is very large in the system, and these packets need to pass through.
Configuration Steps	● Configure the host-based attack threshold.

	Ruijie# configure terminal Ruijie(config)# nfpp Ruijie (config-nfpp)# nd-guard rate-limit per-port ns-na 30 Ruijie (config-nfpp)# nd-guard attack-threshold per-port ns-na 50 Ruijie (config-nfpp)#nd-guard trusted-host 0000.0000.1111
Verification	● Run the **show nfpp nd-guard summary** command to display the configurations.
	(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.) Interface Status Rate-limit Attack-threshold Global Disable 30/15/15
	● Run the **show nfpp nd-guard trusted-host** command to display trusted hosts.
	mac ---- 0000.0000.1111 Total: 1 record(s)

4.4.7 Configuring Centralized Rate Limiting and Distribution

Configuration Effect

Configure centralized rate limiting and distribution so that Manage and Protocol packets are first processed when the network is busy.

Notes

The valid percentage range of a type of packets must be equal to or smaller than (100% – percentage of the sum of the other two types).

Configuration Steps

↘ Configuring the Maximum Bandwidth for Each Type of Packets

- (Mandatory) Manage, Route, and Protocol packets share the same default bandwidth. For details, see the *Product Features*.
- Support the global configuration mode on the AC device.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **pps** *pps_value*
Parameter Description	**manage**: Specifies Manage packets. **protocol**: Specifies Protocol packets. **route**: Specifies Route packets.

	pps_value: Indicates the rate limit, ranging from 1 to 100,000.
Defaults	For the AC devices, the default attack threshold varies with the product model. For the AP devices, the default rate limit of manage, protocol and route packets is 3,000 pps.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the Maximum Percentage of Each Type of Packets in the Queue

- (Mandatory) By default, Manage packets occupy 30% of the bandwidth, Route packets occupy 25%, and Protocol packets occupy 45%.
- Support the global configuration mode on the AC device.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent_value*
Parameter Description	**manage**: Specifies Manage packets. **protocol**: Specifies Protocol packets. **route**: Specifies Route packets. *percent_value*: Indicates the percentage of a type of packets in the queue, ranging from 1 to 100.
Defaults	**manage**: 30% **protocol**: 45% **route**: 25%
Command Mode	Global configuration mode
Usage Guide	The valid percentage range of a type of packets must be equal to or smaller than (100% – percentage of the sum of the other two types).

Configuration Example

Prioritizing Packets Sent to the CPU Through Centralized Distribution

Scenario	● Various types of mass packets exist in the network and belong to different centralized types.
Configuration Steps	● Configure the maximum bandwidth for each type of packets. ● Configure the maximum percentage of each type of packets in the queue.
	`Ruijie# configure terminal` `Ruijie(config)# cpu-protect sub-interface manage pps 5000` `Ruijie(config)# cpu-protect sub-interface manage percent 25`
Verification	Omitted.

4.4.8 Configuring NFPP Log Information

Configuration Effect

NFPP obtains a log from the dedicated log buffer at a certain rate, generates a system message, and clears this log from the dedicated log buffer.

Notes

Logs are continuously printed in the log buffer, even if attacks have stopped.

Configuration Steps

↘ Configuring the Log Buffer Capacity

- Mandatory.
- If the log buffer is full, new logs are discarded and a corresponding prompt is displayed.
- If the log buffer overflows, subsequent logs are discarded and an entry with all attributes marked with a hyphen (-) is displayed in the log buffer. The administrator needs to increase the log buffer capacity or the system message generation rate.
- Support the global configuration mode on the AC device.

Command	**log-buffer entries** *number*
Parameter Description	*number*: Indicates the buffer size in unit of the number of logs, ranging from 0 to 1024.
Defaults	The default buffer size is 256.
Command Mode	NFPP configuration mode
Usage Guide	-

↘ Configuring the System Message Generation Rate

- Mandatory.
- The system message generation rate depends on two parameters: the time segment length and the number of system messages generated in the time segment.
- If both of the preceding two parameters are set to 0, system messages are immediately generated for logs but are not stored in the log buffer.
- Support the global configuration mode on the AC device.

Command	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Parameter Description	*number_of_message*: Ranges from 0 to 1,024. The value 0 indicates that all logs are recorded in the log buffer and no system message is generated. *length_in_seconds*: Ranges from 0 to 86,400 (1 day). The value **0** indicates that logs are not recorded in the log buffer but system messages are instantly generated. This also applies to ***number_of_message*** and ***length_in_seconds***.

	number_of_message/length_in_second: Indicates the system message generation rate.
Defaults	The default value of **number_of_message** is 1 and the default value of **length_in_seconds** is 30.
Command Mode	NFPP configuration mode
Usage Guide	

Enabling Log Filtering

- (Optional) Log filtering is disabled by default.
- Logs can be filtered based on a port or VLAN.
- If log filtering is enabled, logs not meeting the filtering rule are discarded.
- Support the global configuration mode on the AC device.

Command	**logging vlan** *vlan-range*
Parameter Description	*vlan-range*: Records logs in a specified VLAN range. The value format is "1-3,5 for example.
Defaults	All logs are recorded by default.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs in the specified VLAN range are recorded. Between port-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Command	**logging interface** *interface-id*
Parameter Description	*interface-id*: Records logs of a specified port.
Defaults	All logs are recorded by default.
Command Mode	NFPP configuration mode
Usage Guide	Run this command to filter logs so that only logs of the specified port are recorded. Between port-based log filtering and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Configuration Example

CPU Protection Based on ND Guard

Scenario	● If there are too many attackers, log printing will affect the usage of user interfaces and must be restricted.
Configuration Steps	● Configure the log buffer capacity. ● Configure the system message generation rate. ● Configure VLAN-based log filtering.
	`Ruijie# configure terminal`

	Ruijie(config)# nfpp Ruijie (config-nfpp)#log-buffer entries 1024 Ruijie (config-nfpp)#log-buffer logs 3 interval 5 Ruijie (config-nfpp)#logging interface vlan 1
Verification	● Run the **show nfpp log summary** command to display the configurations.
	Total log buffer size : 1024 Syslog rate : 3 entry per 5 seconds Logging: VLAN 1
	● Run the **show nfpp log buffer** command to display logs in the log buffer.
	Protocol VLAN Interface IP address MAC address Reason Timestamp -------- ---- --------- ---------- ---------- ------ --------- ARP 1 Gi0/5 192.168.206.2 001a.a9c2.4609 SCAN 2013-5-1 5:4:24

4.5 Monitoring

Clearing

Description	Command
Clears the ARP guard scanning table.	**clear nfpp arp-guard scan**
Clears monitored hosts in ARP guard.	**clear nfpp arp-guard hosts**
Clears monitored hosts in IP guard.	**clear nfpp ip-guard hosts**
Clears monitored hosts in IMCP guard.	**clear nfpp icmp-guard hosts**
Clears monitored hosts in DHCP guard.	**clear nfpp dhcp-guard hosts**
Clears monitored hosts in DHCPv6 guard.	**clear nfpp dhcpv6-guard hosts**
Clears logs.	**clear nfpp log**

Displaying

Description	Command
Displays configuration parameters of ARP guard.	**show nfpp arp-guard summary**

Description	Command
Displays monitored hosts of ARP guard.	**show nfpp arp-guard hosts**
Displays the ARP guard scanning table.	**show nfpp arp-guard scan**
Displays trusted hosts in ARP guard.	**show nfpp arp-guard trusted-host**
Displays configuration parameters of IP guard.	**show nfpp ip-guard summary**
Displays monitored hosts in IP guard.	**show nfpp ip-guard hosts**
Displays trusted hosts in IP guard.	**show nfpp ip-guard trusted-host**
Displays configuration parameters of ICMP guard.	**show nfpp icmp-guard summary**
Displays monitored hosts in ICMP guard.	**show nfpp icmp-guard hosts**
Displays trusted hosts in ARP guard.	**show nfpp icmp-guard trusted-host**
Displays configuration parameters of DHCP guard.	**show nfpp dhcp-guard summary**
Displays monitored hosts in DHCP guard.	**show nfpp dhcp-guard hosts**
Displays trusted hosts in DHCP guard.	**show nfpp dhcp-guard trusted-host**
Displays configuration parameters of DHCPv6 guard.	**show nfpp dhcpv6-guard summary**
Displays monitored hosts in DHCPv6 guard.	**show nfpp dhcpv6-guard hosts**
Displays trusted hosts in DHCPv6 guard.	**show nfpp dhcpv6-guard trusted-host**
Displays configuration parameters of ND guard.	**show nfpp nd-guard summary**
Displays trusted hosts in ND guard.	**show nfpp nd-guard trusted-host**
Displays NFPP logs.	**show nfpp log summary**
Displays the NFPP log buffer.	**show nfpp log buffer** [**statistics**]

5 Configuring WAPI

5.1 Overview

WLAN Authentication and Privacy Infrastructure (WAPI) is a wireless network security standard for which China has the proprietary intellectual property rights.

WAPI comprises two parts:

- WLAN Authentication Infrastructure (WAI): a security solution used for identification and key management in a WLAN. WAPI provides two authentication approaches: WAPI pre-shared key authentication and WAPI certificate authentication.
- WLAN Privacy Infrastructure (WPI): a security solution used for data transfer protection in a WLAN, including data encryption, data authentication and replay prevention.

WAPI can be applied in both small- and large-scaled WLANs. The pre-shared key authentication is a simple authentication mechanism not requiring dedicated authentication servers. However, the WAPI certificate authentication needs to use dedicated servers and can be used to provide secure and easy-to-manage access solutions for large-scaled WLANs.

Protocols and Standards

- GB 15629.11-2003/XG1-2006: Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 1
- RFC 3280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4492:Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
- WAPI Multi-trust Certificate Implementation Technology, a technical guide for multi-certificate authentication

5.2 Applications

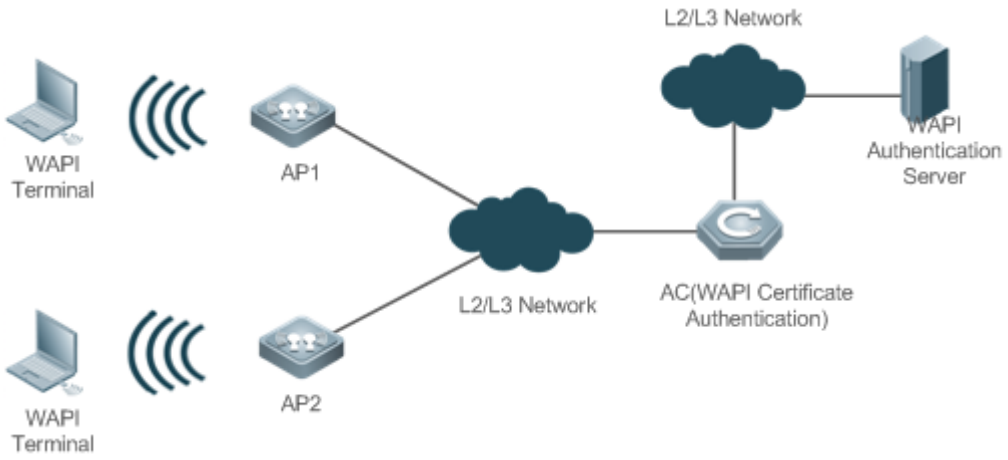
Application	Description
WAPI Certificate Authentication	In large-scaled WLANs, it is recommended to configure the WAPI certificate authentication mode.
WAPI Pre-shared Key Authentication	In small-scaled WLANs or those not requiring management, you can configure the WAPI pre-shared key authentication mode.

5.2.1 WAPI Certificate Authentication

Scenario

In large-scaled WLANs, it is recommended to configure the WAPI certificate authentication mode. Figure 5-1 shows a typical scenario.

Figure 5-1



Deployment

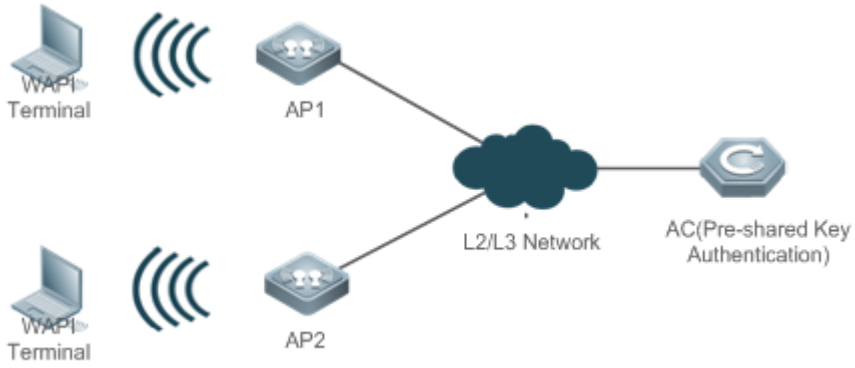
- Configure a WLAN on the AC.
- Configure a server for WAPI certificate authentication.
- Configure the WAPI certificate authentication mode in the WLAN security configuration mode.
- Push the WLAN to the AP.

5.2.2 WAPI Pre-shared Key Authentication

Scenario

In small-scaled WLANs or those not requiring management, you can configure the WAPI pre-shared key authentication mode. Figure 5-2 shows a typical scenario.

Figure 5-2



Deployment

- Configure a WLAN on the AC.
- Configure the PSK certificate authentication approach in the WLAN security configuration mode.

- Push the WLAN to the AP.
- Use this authentication with the WEB authentication to support web-based authentication and charging.

5.3 Features

Basic Concepts

AE

Authenticator Entity: An entity that provides authentication service for the ASUE before the ASUE accesses a service. This entity resides in the AP or AC.

AS

Authentication Server: The AS provides the WAPI certificate authentication service.

ASU

Authentication Service Unit: An entity that provides mutual authentication service for the AE and ASUE. This entity resides in the AS.

ASUE

Authentication Supplicant Entity: An entity that requests authentication before accessing a service. This entity resides in the STA.

BK

Base Key: A key used for exporting unicast session keys. A BK is obtained through negotiation during certificate authentication or is exported from a pre-shared key.

CA

Certification Authority: A CA is a trusted third-party organization who ensures that a certificate is issued to a person who deserves it.

Overview

Feature	Description
WAPI Authentication Approaches	You can enable authentication for an STA that accesses a WLAN.
WAPI Key Management	You can enable unicast key negotiation and multicast key announcement.

5.3.1 WAPI Authentication Approaches

WAPI defines two authentication approaches:

- Certificate authentication
- Pre-shared key authentication

Working Principle

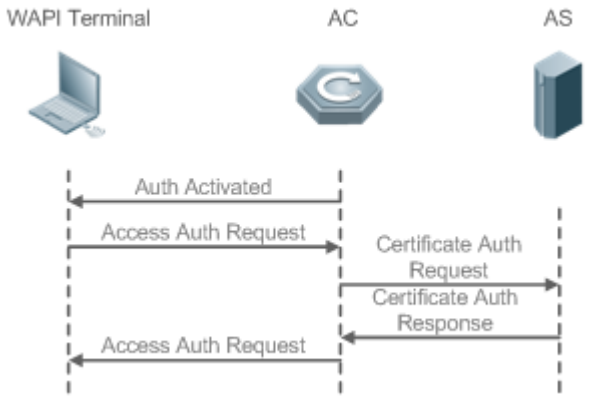
Certificate Authentication

Certificate authentication refers to authentication based on the certificates of an STA and an AE. Before authentication, the STA and AE must have their own certificates. Then, the AS is used to authenticate the STA and AE to generate a BK based on their temporary public keys and private keys and prepare for subsequent unicast key negotiation and multicast key announcement.

When the WAPI function is applied in large-scaled WLANs, the certificate issuing system and certificate authentication system must be separated. The ASUE and AE should be installed with three certificates: user or STA certificate, CA certificate, and trusted ASU certificate. Among them, the ASU certificate is a mandatorily trusted certificate. After the certificates are installed, the ASUE and AE become the CA and ASU. Therefore, we call this mode WAPI three-certificate authentication mode. If the certificate issuing system and certificate authentication system are the same entity, this mode is called WAPI two-certificate authentication mode.

Figure 5-3 shows the certificate authentication process.

Figure 5-3



Remarks	AC is the AE equipment. Auth is short for authentication.

Pre-shared Key Authentication

Pre-shared key authentication refers to authentication based on the keys of an STA and an AE. Before authentication, the STA and AE must be configured with the same key, namely, a pre-shared key. During authentication, the pre-shard key is directly converted into a BK, and then unicast key negotiation and multicast key are announced.

5.3.2 WAPI Key Management

The unicast data between the STA and AE are protected by unicast encryption key and unicast integrity check key obtained through negotiation during the unicast key negotiation. The AE protects sent broadcast/multicast data by using the multicast encryption key and multicast integrity check key announced by itself and exported from the multicast primary key. On the other hand, the STA decrypts received broadcast/multicast data by using the multicast encryption key and multicast integrity check key announced by the AE and exported from the multicast primary key.

Working Principle

Unicast Key Negotiation

Unicast key negotiation is performed first. Figure 5-4 shows the negotiation process.

Figure 5-4

After the certificate authentication succeeds, the AE sends a key negotiation request to the ASUE, containing the key negotiation request data.

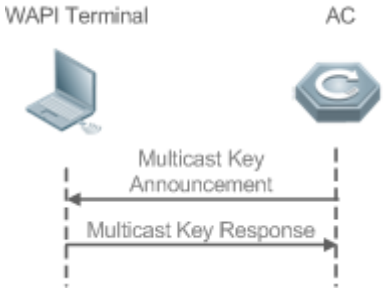
After receiving the unicast key negotiation request and verifying the validity of the request, the ASUE generates key negotiation response data, constructs a unicast key negotiation response and sends the response to the AE. The ASUE and AE generate a unicast session key by using the key negotiation data.

After receiving the unicast key negotiation response and verifying the validity of the response, the AE sends a unicast key negotiation ACK message to the ASUE. In this way, the ASUE and AE establish a unicast key security association.

Multicast Key Announcement

After unicast key negotiation is completed, the key obtained through the unicast key negotiation is used to announce a multicast key. Figure 5-5 shows the announcement process.

Figure 5-5



After the unicast key negotiation succeeds, that is, a unicast key security association is established, the AE sends a multicast key announcement to the ASUE to notify the ASUE of the key used by the AE for sending multicast data.

After verifying the validity of the multicast key announcement sent by the AE, the ASUE sends a multicast key response to the AE. In this way, the ASUE and AE establish a multicast key security association.

In both WAPI certificate authentication and pre-shared key authentication approaches, the key interaction is performed for an STA to access a WLAN.

5.4 Configuration

Configuration	Description and Command	
Configuring WAPI Certificate Authentication	(Mandatory) It is used to enable the WAPI certification authentication approach.	
	security wapi	Configures and enables the WAPI security mode
	security wapi ae cert	Configures the WAPI certificate of the AE equipment
	security wapi asu address	Configures the IP address of the authentication server
	security wapi ca cert	Configures a CA certificate
	(Optional) It is used to enable the WAPI two-certificate or three-certificate authentication mode. After the WAPI certificate authentication mode is enabled, you should specify either the two-certificate or three-certificate authentication mode.	
	security wapi 2-cert	Configures the two-certificate authentication mode
	security wapi 3-cert	Configures the three-certificate authentication mode
	security wapi asu cert	Configures the WAPI certificate for the authentication server
Configuring WAPI Pre-shared Key Authentication	(Mandatory) It is used to enable the WAPI pre-shared key authentication approach.	
	security wapi	Configures and enable the WAPI security mode.
	security wapi psk	Configures and enables the WAPI pre-shared key authentication approach.
	security wapi psk set-key	Configures a WAPI pre-shared key.

5.4.1 Configuring WAPI Certificate Authentication

Configuration Effect

- Enable the WAPI certificate authentication approach and use the certificate authentication approach to authenticate an STA that accesses a WLAN.
- Configure either the two-certificate or three-certificate authentication mode.

Notes

- In the security configuration mode of a WLAN, the two-certificate and three-certificate authentication modes cannot be enabled at the same time.
- The certificate authentication mode must work with the WAPI authentication server.

Configuration Steps

↘ **Enabling the WAPI Security Mode**

- Mandatory.

- It is configured in the WLAN security configuration mode on the AC.

Command	**security wapi** { **enable** | **disable** }
Parameter Description	**enable**: Enables the WAPI security mode. **disable**: Disables the WAPI security mode.
Defaults	Disabled
Command Mode	WLAN security configuration mode
Usage Guide	In the security configuration mode of a WLAN, the WAPI security mode cannot be enabled together with other encryption and authentication modes.

Configuring the Two-Certificate Authentication Mode

- Optional. It is configured when you want to enable the WAPI two-certificate authentication mode. The **security wapi 2-cert { enable | disable }** command can be used to enable or disable the WAPI two-certificate authentication mode.
- It is configured in the WLAN security configuration mode on the AC.
- Before configuring the two-certificate authentication mode, enable the WAPI security mode. In the security configuration mode of a WLAN, the two-certificate and three-certificate authentication modes cannot be enabled at the same time. After the WAPI two-certificate authentication mode is configured, the STA accesses the WLAN by using the two-certificate authentication mode.

Command	**security wapi 2-cert** { **enable** | **disable** }
Parameter Description	**enable**: Enables the WAPI two-certificate authentication. **disable**: Disables the WAPI two-certificate authentication.
Defaults	Disabled
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the two-certificate authentication mode, enable the WAPI security mode. In the security mode of a WLAN, the two-certificate and three-certificate authentication modes cannot be enabled at the same time.

Configuring the Three-Certificate Authentication Mode

- Optional. It is configured when you want to enable the WAPI three-certificate authentication mode. The **security wapi 3-cert { enable | disable }** command can be used to enable or disable the WAPI three-certificate authentication mode.
- It is configured in the WLAN security configuration mode on the AC.
- Before configuring the three-certificate authentication mode, enable the WAPI security mode. In the security configuration mode of a WLAN, the two-certificate and three-certificate authentication modes cannot be enabled at the same time. After the WAPI three-certificate authentication mode is configured, the STA accesses the WLAN by using the three-certificate authentication mode.

Command	**security wapi 3-cert** { **enable** | **disable** }
Parameter Description	**enable**: Enables the WAPI three-certificate authentication. **disable**: Disables the WAPI three-certificate authentication.

Defaults	Disabled
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the three-certificate authentication mode, enable the WAPI security mode. In the security configuration mode of a WLAN, the two-certificate and three-certificate authentication modes cannot be enabled at the same time.

Configuring the WAPI Certificate of the AE

- Mandatory.
- It is configured in the WLAN security configuration mode on the AC.

Command	**security wapi ae cert** *ae_certfile*
Parameter Description	*ae_certfile*: Specifies the WAPI certificate file name of the AE
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the AE certificate, enable the WAPI security mode. Before configuration, ensure that the certificate file is imported into the AE and ASUE.

Configuring the IP Address of the Authentication Server

- Mandatory.
- It is configured in the WLAN security configuration mode on the AC.

Command	**security wapi asu address** *ip_address*
Parameter Description	*ip_address*: Specifies the IP address of the authentication server.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the IP address of the authentication server, enable the WAPI security mode.

Configuring the WAPI Certificate for the Authentication Server

- Optional. The ASU certificate must be configured for the three-certificate authentication mode.
- It is configured in the WLAN security configuration mode on the AC.

Command	**security wapi asu cert** *asu_certfile*
Parameter Description	*asu_certfile*: Specifies the ASU certificate file name.
Defaults	N/A
Command Mode	WLAN security configuration mode

Usage Guide	Before configuring the ASU certificate, enable the WAPI security mode. Before configuration, ensure that the certificate file is imported into the AE and ASUE. The ASU certificate must be configured for the three-certificate authentication mode. The ASU certificate does not need to be configured in the two-certificate authentication mode.

Configuring a CA Certificate

- Mandatory.
- It is configured in the WLAN security configuration mode on the AC.

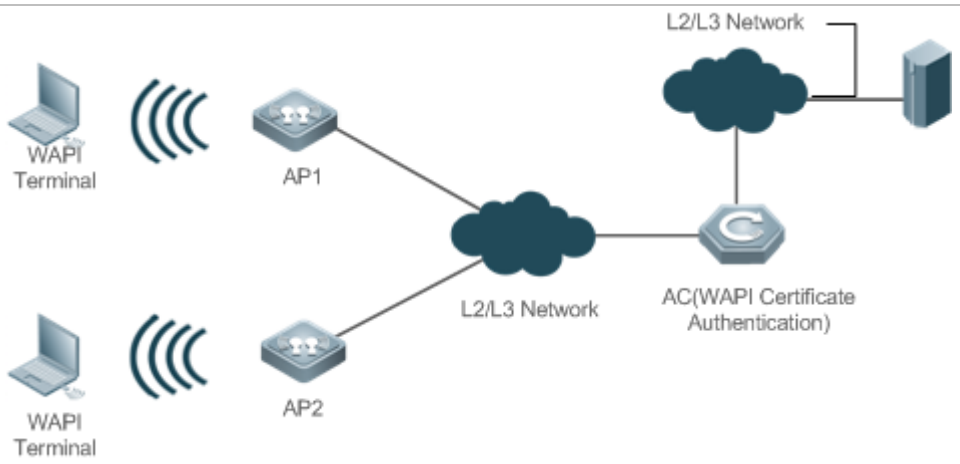
Command	**security wapi ca cert** *ca_certfile*
Parameter Description	*ca _certfile*: Specifies the CA certificate file name.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the CA certificate, enable the WAPI security mode. Before configuration, ensure that the certificate file is imported into the AE and ASUE.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

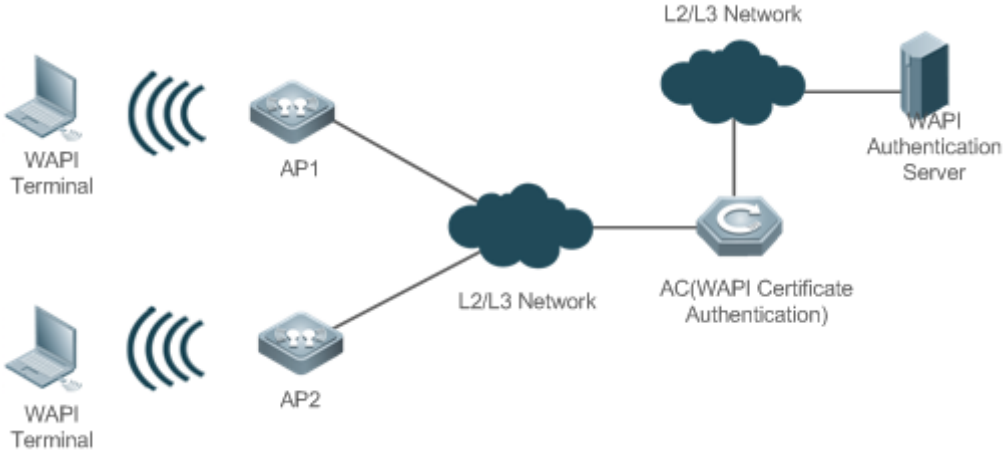
Configuration Example

Configuring the WAPI Two-Certificate Authentication Mode for WLAN 1

Scenario **Figure 5-6**	 The IP address of the authentication server is 192.168.1.123.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable the WAPI security mode. ● Enable the two-certificate authentication mode. ● Configure a CA certificate.

	● Configure the WAPI certificate of the AE. ● Configure the IP address of the authentication server.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security wapi enable` `Ruijie(config-wlansec)#security wapi 2-cert enable` `Ruijie(config-wlansec)#security wapi ca cert CA.cer` `Ruijie(config-wlansec)#security wapi ae cert AE.cer` `Ruijie(config-wlansec)#security wapi asu address 192.168.1.123`
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config | begin wlansec 1` `wlansec 1` `security wapi enable` ` security wapi asu address 192.168.1.123` ` security wapi ca cert CA.cer` ` security wapi ae cert AE.cer` ` security wapi 2-cert enable` `!`

Configuring the WAPI Three-Certificate Authentication Mode for WLAN 1

Scenario **Figure 5-7**	 The IP address of the authentication server is 192.168.1.123.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable the WAPI security mode. ● Enable the three-certificate authentication mode. ● Configure a CA certificate. ● Configure the WAPI certificate of the AE. ● Configure the WAPI certificate for the authentication server. ● Configure the IP address of the authentication server.

AC	Ruijie(config)#wlansec 1 Ruijie(config-wlansec)#security wapi enable Ruijie(config-wlansec)#security wapi 3-cert enable Ruijie(config-wlansec)#security wapi ca cert CA.cer Ruijie(config-wlansec)#security wapi ae cert AE.cer Ruijie(config-wlansec)#security wapi asu cert ASU.cer Ruijie(config-wlansec)#security wapi asu address 192.168.1.123
Verification	Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	Ruijie#show running-config | begin wlansec 1 wlansec 1 security wapi enable security wapi asu address 192.168.1.123 security wapi asu cert ASU.cer security wapi ca cert CA.cer security wapi ae cert AE.cer security wapi 3-cert enable !

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP/RSN/WPA).
- The three-certificate authentication mode is enabled before WAPI security mode.
- The WAPI certificate is not imported into the equipment.

5.4.2 Configuring WAPI Pre-shared Key Authentication

Configuration Effect

- To enable the WAPI pre-shared key authentication, the STA and AE must be configured with the same key in advance.

Notes

- After the WAPI pre-shared key authentication mode is enabled, a pre-shared key must be configured.

Configuration Steps

↘ Enabling the WAPI Security Mode

- Mandatory.
- It is configured in the WLAN security configuration mode on the AC.

Command	**security wapi** { **enable** | **disable** }
Parameter	**enable**: Enables the WAPI security mode.

Description	**disable**: Disables the WAPI security mode.
Defaults	Disabled
Command Mode	WLAN security configuration mode
Usage Guide	In the security configuration mode of a WLAN, the WAPI security mode cannot be enabled together with other encryption and authentication modes.

Enabling the WAPI Pre-shared Key Authentication Approach

- Mandatory. The **security wapi psk { enable | disable }** command can be used to enable or disable the WAPI pre-shared key authentication mode.
- It is configured in the WLAN security configuration mode on the AC .
- Before configuring the WAPI pre-shared key authentication mode, enable the WAPI security mode. The STA can access the WLAN configured with the WAPI pre-shared key authentication only after you input the same pre-shared key as that on the AE.

Command	**security wapi psk** { **enable** | **disable** }
Parameter Description	**enable**: Enables the WAPI pre-shared key authentication mode. **disable**: Disables the WAPI pre-shared key authentication mode.
Defaults	Disabled
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the WAPI pre-shared key authentication approach, enable the WAPI security mode.

Configuring a WAPI Pre-shared Key

- Mandatory.
- It is configured in the WLAN security configuration mode on the AC.

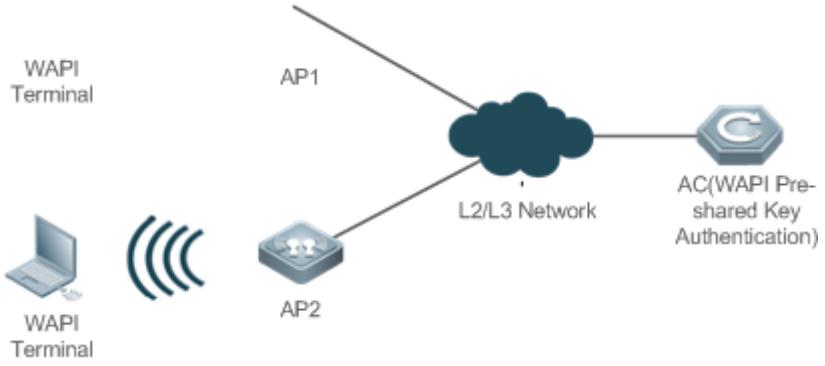
Command	**security wapi psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the pre-shared key is in the ASCII format. *ascii-key*: Specifies a key consisting of 8-32 ASCII characters. **hex**: Specifies that the pre-shared key is in the hexadecimal format. *hex-key*: Specifies a key consisting of 16-64 hexadecimal characters. The length must be an even number.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	Before configuring the WAPI pre-shared key, enable the WAPI security mode. The key consists of 8-32 ASCII characters.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring the WAPI Pre-shared Key Authentication Approach for WLAN 1 with the Key of 12345678

Scenario **Figure 5-8**	
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable the WAPI security mode. ● Enable the WAPI pre-shared key authentication mode. ● Set the WAPI pre-shared key to 12345678.
AC	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security wapi enable` `Ruijie(config-wlansec)#security wapi psk enable` `Ruijie(config-wlansec)#security wapi psk set-key ascii 12345678`
Verification	Run the **show running-config	begin wlansec** *wlan_id* command to check whether the configuration takes effect.
AC	`Ruijie#show running-config	begin wlansec 1` `wlansec 1` ` security wapi enable` ` security wapi psk set-key ascii 12345678` ` security wapi psk enable` `!`

Common Errors

- The WLAN has been enabled with other encryption and authentication modes (such as WEP/RSN/WPA).
- The WAPI pre-shared key contains less than 8 or more than 32 ASCII characters.

5.5 Monitoring

Displaying

Description	Command
Displays WAPI user status.	**show wapi-sta summary**

WLAN QoS Configuration

1. Configuring WLAN QoS
2. Configuring WMM
3. Configuring VIP-FIRST

1 Configuring WLAN QoS

1.1 Overview

WLAN QoS (WQoS) is a wireless bandwidth control technology. It involves rate limiting and fair scheduling.

Rate limiting is used to limit the traffic of access points (APs), WLAN, or STAs, thus preventing the traffic from exceeding a specified range. Rate limiting is applicable to scenarios where some STAs occupy too much bandwidth and other STAs do not have sufficient bandwidth.

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes. Fair scheduling is applicable to all wireless networks.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- Wi-Fi: WMM Specification version 1.1

1.2 Applications

Application	Description
Bandwidth Control in a Fit AP Architecture	A fit AP architecture is deployed with at least one access controller (AC) and one AP.

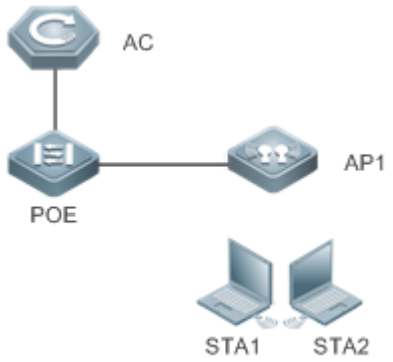
1.2.1 Bandwidth Control in a Fit AP Architecture

Scenario

On the wireless network, an AC is deployed to implement rate limiting on APs, WLANs, and STAs, and fair scheduling on APs.

As shown in Figure 1-1, the AC implements rate limiting on APs, WLANs, and STAs, and fair scheduling on APs.

Figure 1-1



Remarks	AC: Wireless access controller POE: Gateway switch for AP 1 AP 1:Wireless access device STA 1 and STA 2: User devices

Deployment

- Enable WQoS on the AC.

1.3 Features

Basic Concepts

Rate Limiting

To better utilize the limited network resources and serve more users efficiently, the access device need to support rate limiting. When the traffic rate conforms to the committed rates, packets are allowed to pass; otherwise, packets are discarded.

The following parameters are used to evaluate the traffic:

- Average Data Rate: It is the average flow rate that is allowed. It is also called committed information rate (CIR).
- Burst Data Rate: It is the maximum acceptable rate of each burst data, also called committed burst size (CBS).The configured CBS must be greater than the maximum packet length, that is, the maximum rate at which data is sent in a period of 10 milliseconds. (The CBS in the unit of Kbps is equal to the maximum traffic in a period divided by 10 milliseconds).

Fair Scheduling

Fair scheduling allows STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP fairly. The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs. Besides, the fair scheduling function provides users with better experience by monitoring changes in the traffic of each STA intelligently and adjusting the proportion of the

wireless bandwidth used by each STA dynamically. In software version later than 10.4(1T19)p1, different priorities can be configured for STAs in fair scheduling so that specified users can preferentially enjoy the wireless bandwidth.

Overview

Feature	Description
Rate Limiting	Limit the rates of an AP, a WLAN, or a STA to that the rate does not exceed the limit.
Fair Scheduling	Associate a STA with other STAs in the same frequency band of the same AP to share the wireless network resources provided by the AP, thus sharing the bandwidth of the wireless network in a fair manner.

1.3.1 Rate Limiting

Rate limiting is used to limit the rates of an AP, a WLAN, or a STA to ensure that the rate does not exceed a certain range.

Working Principle

Rate limiting is implemented based on the token bucket.

- The token bucket records the number of bytes that can pass in a certain period of time.
- In each period, the number of data bytes that can pass is calculated based on the configured CIR and CBS, thereby adjusting the size of the token bucket.
- When a packet arrives, the packet size in bytes is compared with the size of the token bucket. When the packet size is smaller than that of the token bucket, the packet is allowed to pass, and the token bucket size decreases with the corresponding amount. When the packet size is greater than that of the token bucket, two processing methods are followed: the packet is directly dropped. Traffic Policing results in big fluctuation of traffic.
- On an AC, Traffic Policing is used to implement rate limiting of a WLAN.

1.3.2 Fair Scheduling

Fair scheduling, by dividing the time equally, resolves the problem that some nodes occupy the air interfaces for a longer time, particularly low-rate nodes.

Working Principle

Owing to the special characteristics of the wireless network, STAs (including APs) on the same network share the air interface resources, which is also a bottleneck of STA performance. This is one of the differences between the wired and wireless networks. Traditional packet scheduling often adopts the first in first out (FIFO) mode. On one wireless network, every STA that needs to transmit data want to occupy the air interface resources whenever possible. Transmission of overwhelming low-rate packets results in long-time occupation of the air interfaces. Thereby, the lasting queue take-up causes packet loss and degrades the overall performance of the network.

In the real wireless scenarios, STAs often differ in types and performance. Consequently, some STAs always cannot obtain the resources, or get super slow response. What is worse, these STAs cannot access the network, which seriously affects user experience.

To settle the problems, it is essential to ensure that each STA is able to obtain resources on air interfaces fairly. That is, every STA that needs to transmit data can occupy the air interfaces for a fair period of time. Fair scheduling of the wireless links can be achieved by ways as follows: Predict the traffic of every STA based on the STA-specific information (such as negotiated rates and aggregation types) and the valid bytes of packets, convert the traffic to the number of packets that can be transmitted by every STA, and adjust the allowed packet number to allocate the bandwidth to every STA over the air interfaces and implement traffic shaping. With fair scheduling, each STA occupies the air interfaces for an equal period of time, which effectively avoids poor performance of some STAs and thus improves user experience.

1.4 Configuration

Configuration	Description and Command	
Configuring Rate Limiting	(Mandatory) It is used to enable rate limiting.	
	ap-based	Configures AP-based rate limiting on an AC.
	netuser	Configures STA-based rate limiting on an AC.
	wlan-based	Configures WLAN-based rate limiting on an AC.
Configuring Fair Scheduling	(Mandatory) It is used to enable fair scheduling.	
	fair-schedule	Enables fair scheduling.
	(Optional) It is used to adjust the STA priority during fair scheduling.	
	sta-fair	Configures the fair scheduling priority of a STA.

1.4.1 Configuring Rate Limiting

Configuration Effect

- Only the committed resource is allocated to a stream based on the actual situation of the network, which prevents network congestion caused by burst stream.

Notes

- The rate limiting effect of the **wlan-based per-ap-limit** command configured on an AC is equivalent to that of the **wlan-qos wlan-based total-user-limit** command configured on all connected APs.
- The following types of rate limiting are available on STAs: **wlan-based per-user-limit**, **wlan-based per-ap-limit intelligent**, **ap-based per-user-limit**, **ap-based total-limit intelligent**, and **netuser**. However, only one type of them works at a time. From high to low, the priorities of these types of rate limiting are as follows: **netuser**>**wlan-based per-ap-limit intelligent** > **wlan-based per-user-limit** > **ap-based total-limit intelligent** > **ap-based per-user-limit**.
- Rate limiting, including **wlan-based total-limit**, **wlan-based per-ap-limit**, **ap-based total-limit**, and STA-based rate limiting, can take effect on different objects simultaneously without considering priorities.

Configuration Steps

Configuring AP-based Rate Limiting

- Mandatory.
- On an AC, run the **wlan-qos ap-based** command in AP configuration mode to configure AP-based rate limiting.

Command	**wlan-qos ap-based** { **per-user-limit** | **total-user-limit** [**intelligent**] } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Indicates that rate limiting is implemented on every STA on the AP. **total-user-limit**: Indicates that rate limiting is implemented on all STAs on the AP. **intelligent**: Indicates whether rate limiting is implemented on all STAs on the AP intelligently. **down-streams**: Indicates that rate limiting is implemented on the downlink traffic of the AP. **up-streams**: Indicates that rate limiting is implemented on the uplink traffic of the AP. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured. If **total-user-limit** is configured, intelligent rate limiting is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring STA-based Rate Limiting

- Mandatory.
- On an AC, run the **wlan-qos netuser** command in AC configuration mode to configure STA-based rate limiting.

Command	**wlan-qos netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: Indicates the MAC address of a STA. **inbound:** Indicates that rate limiting is implemented on the uplink traffic of a STA. **outbound:** Indicates that rate limiting is implemented on the downlink traffic of a STA. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring WLAN-based Rate Limiting

- Mandatory.
- On an AC, run the **wlan-based** command in WLAN configuration mode to configure WLAN-based rate limiting.

Command	**wlan-based** { **per-user-limit** | **total-user-limit** [**intelligent**] | **per-ap-limit** } { **down-streams** | **up-streams** }

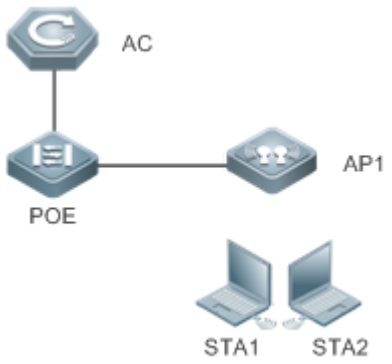
	average-data-rate *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Indicates that rate limiting is implemented on every STA on the WLAN. **total-user-limit**: Indicates that rate limiting is implemented on all STAs on the WLAN. **intelligent**: Indicates whether rate limiting is implemented on all STAs on the WLAN intelligently. **per-ap-limit**: Indicates that AP-based rate limiting is implemented. **down-streams**: Indicates that rate limiting is implemented on the downlink traffic of the WLAN. **up-streams**: Indicates that rate limiting is implemented on the uplink traffic of the WLAN. *average-data-rate*: Indicates CIR. The unit is 8 Kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Indicates CBS. The unit is 8 Kbps. The value ranges from 8 to 261,120.
Defaults	By default, rate limiting is not configured.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show dot11 ratelimit ap** command to display the AP-based rate limiting information.
- Run the **show dot11 ratelimit user** command to display the STA-based rate limiting information.
- Run the **show dot11 ratelimit wlan** command to display the WLAN-based rate limiting information.

Configuration Example

Configuring AP-based Rate Limiting

Scenario Figure 1-2	
Configuration Steps	● In AP configuration mode, configure AP-based, STA-based, and downlink rate limiting.

AC	Ruijie#configure terminal Ruijie(config)# ap-config ap1 Ruijie(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000 Ruijie(config-ap)# exit
Verification	Run the **show dot11 ratelimit ap** command to display the configurations.
AC	AC_20_3F#show dot11 ratelimitap AP name :test, ratelimit info(unit :8kbps): Per-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream : average rate - 100000, burst rate - 120000 Total-user-limit: Upstream : average rate - 0 , burst rate - 0 Downstream : average rate - 0 , burst rate - 0

1.4.2 Configuring Fair Scheduling

Configuration Effect

- The fair scheduling function can prevent low-speed STAs from decreasing the throughput of the entire wireless network, and provide smoother network experience for STAs.

Notes

- In fit AP mode, configure fair scheduling only on an AC.

Configuration Steps

↘ Enabling Fair Scheduling

- Mandatory.
- On an AC, run the **fair-schedule** command in AP configuration mode to enable fair scheduling.
- Enabling fair scheduling can allocate time to STAs in a fair manner.

Command	**fair-schedule**
Parameter Description	N/A
Defaults	By default, fair scheduling is enabled.
Command Mode	AP configuration mode

Usage Guide	N/A

Configuring the Fair Scheduling Priority

- (Optional) Perform this configuration if you need to change the fair scheduling priority of a STA.
- On an AC, run the **sta-fair** command in AC configuration mode to configure the fair scheduling priority.

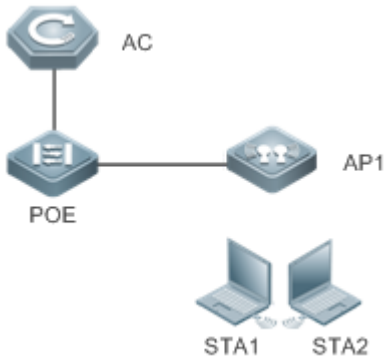
Command	**sta-fair** *mac-address* **priority** *priority*
Parameter Description	*mac-address*: Indicates the MAC address of a STA. *priority*: Indicates the priority. The value ranges from 1 to 6.
Defaults	By default, the priority is 1 for all STAs. A greater value indicates a higher priority, and a higher priority indicates that a longer time is allocated to the STA.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config run** command to display the configurations.

Configuration Example

Enabling Fair Scheduling and Configuring the Priority

Scenario Figure 1-3	
Configuration Steps	● In AP configuration mode, enable fair scheduling. ● In AC configuration mode, configure the fair scheduling priority of a STA.

AC	Ruijie#configure terminal Ruijie(config)# ap-config ap1 Ruijie(config-ap)#fair-schedule Ruijie(config-ap)# exit Ruijie(config)#ac-controller Ruijie(config-ac)#sta-fair 1111.1111.1111 priority 6 Ruijie(config-ac)# end
Verification	Run the **show ap-config running** and **show running-config** commands to display the configurations.
AC	Ruijie# show ap-config running ! ap-configap1 ! Ruijie# show running-config ! ac-controller sta-fair 1111.1111.1111 priority 6 !

1.5 Monitoring

Displaying

Description	Command
Displays the WQoS rate limiting information.	**show dot11 ratelimit** {**wlan** | **ap** | **user** }

2 Configuring WMM

2.1 Overview

WMM is a wireless QoS protocol, and this protocol is a subset of the 802.11e protocol.

WMM is used to ensure that high-priority packets are preferentially sent, thereby assuring the quality of the voice and video applications in a wireless network.

This document consists of two parts, that is, WMM service and QoS packet priority mapping.

- WMM service: The WMM service is used to differentiate the capabilities of the access channels with different priorities, thereby ensuring that channel resources are allocated based on data flow priorities. Users can adjust the values of the EDCA parameters for the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
- QoS packet priority mapping: Wireless-to-Wired QoS mapping and wired-to-wireless QoS mapping help to implement end-to-end QoS in the entire network, thereby assuring the quality of high-priority service flows.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE802.11

2.2 Applications

Application	Scenario
WMM Service Scenario	Competition process of channels with different priorities.
Wireless-to-Wired Priority Mapping Scenario	Wireless-to-wired QoS packet priority mapping process.
Wired-to-Wireless Priority Mapping Scenario	Wired-to-wireless QoS packet priority mapping process.

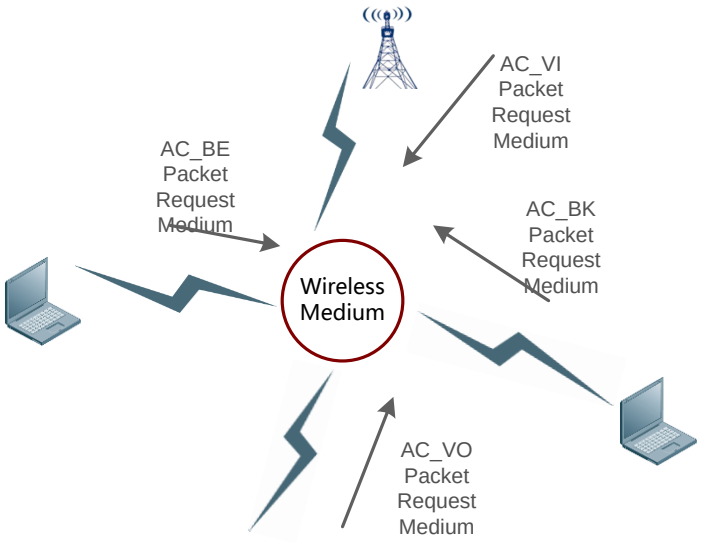
2.2.1 WMM Service

Scenario

The medium for wireless communication is radio. In a specified frequency band, channels are shared during wireless network communication. In the same RF environment, the uplink and downlink traffic of different sites conflicts. Therefore, the problem how communication participants compete for shared channels needs to be solved to ensure wireless QoS. As shown in Figure 2-1, there are packets of four different priorities in the same wireless network environment (the packets from high priority to low are as follows: AC_VO > AC_VI > AC_BE > AC_BK). When multiple supplicants request the medium to

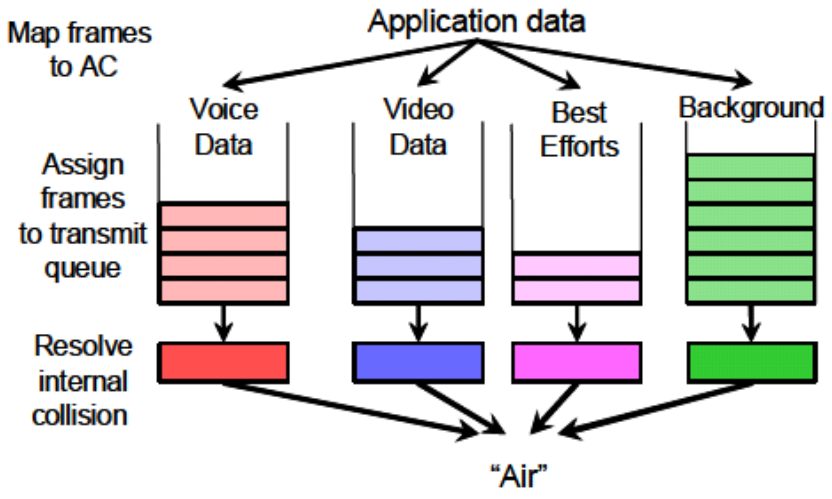
send packets and compete for channels, the competition and coordination mechanism is enabled to determine which supplicant's packet can access the medium. The higher the packet's priority is, the more likely the packet is to access the channel.

Figure 2-1 Channel competition



In a wireless network, since the medium is special, packet damage caused by packet loss and signal interference occurring during transmission over the network is quite serious. Different wireless transmission parameters of the mechanism need to be retransmitted to ensure arrival of packets. However, it is unpractical that preferable parameters are adopted for all packets. In this case, to provide services having high reliability and timeliness requirements, you can classify packets. In short, provide network services of different quality based on various requirements. That is, process key data packets having high timeliness requirement preferentially, and assign a low processing priority to general packets not having high timeliness requirement. To make a network carry different services, you must ensure that the network not only provides single service with the best QoS, but also provides different service with different QoS. Therefore, the QoS of a wireless AP requires the classification/identification of packets for identifying different data flows and providing service of different quality.

Figure 2-2 Wireless QoS multi-priority queue



Deployment

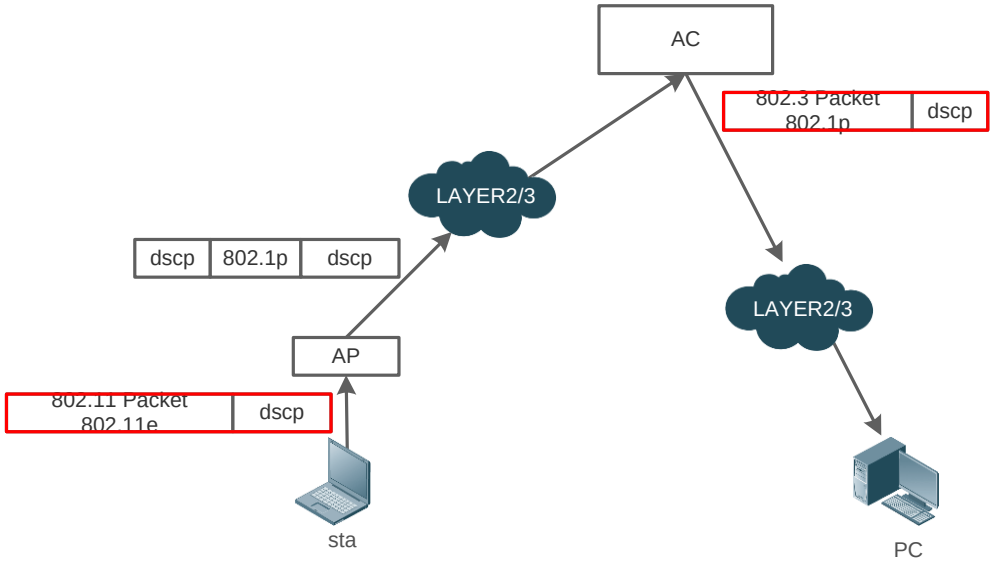
The device should be configured with the following key points:

- Enable the WMM.
- Set WMM EDCA competition parameters. Generally, default values are adopted.

2.2.2 Wireless-to-Wired Priority Mapping

Scenario

Figure 2-3 Wireless-to-wired packet priority mapping



STA-to-PC priority mapping process:

- STA sends an 802.11 packet carrying 802.11e and DSCP information to the AP.

- The AP sets the internal priority of the packet based on the trust mode of the wireless port (configured on the ESS of the AC based on the BSSID). If the trusted packet is with an 802.11e priority, the AP converts the packet with the 802.11e priority into a wired packet with the 802.1p and DSCP priorities and a CAPWAP encapsulated packet with the 802.1p and DSCP priorities. If the trust mode is DSCP priority, the preceding setting shall be performed based on the DSCP priority of the incoming wireless packet. Currently, the default ETH trust mode is DSCP, and the wireless end always maps to the dot11e.
- When passing layer 2/3 network, the CAPWAP packet is processed according to the wired QoS method.
- After receiving the CAPWAP packet, the AC decapsulates the packet and then forwards the wired packet generated after the decapsulation to the layer 2/3 network.
- When passing layer 2/3 network, the wired packet is processed according to the wired QoS method.

Deployment

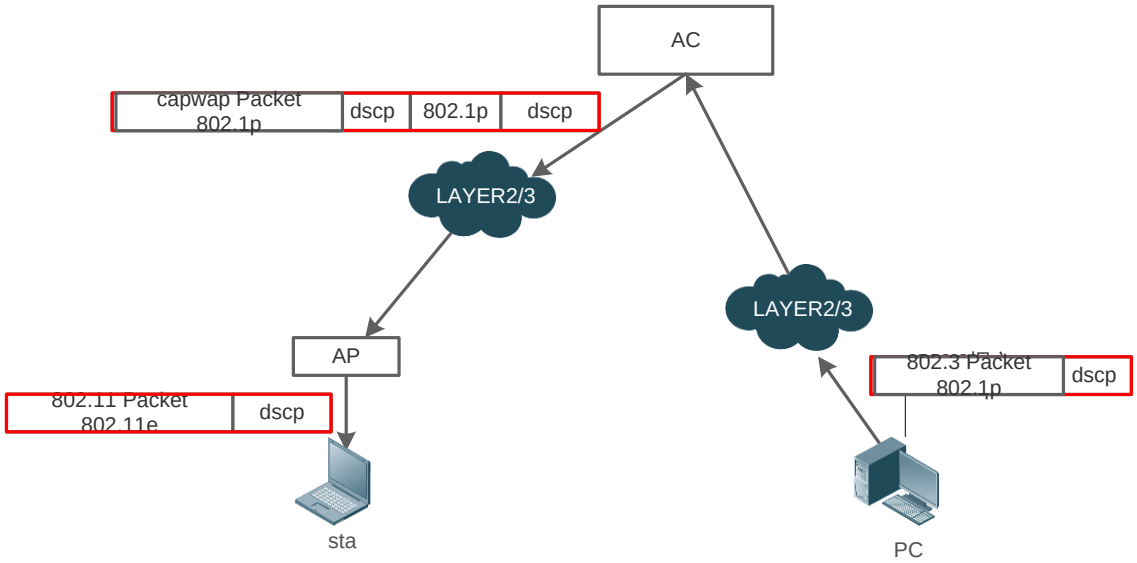
The device should be configured with the following key points:

- Enable the WMM.
- Set the wireless-to-wired priority mapping table. Generally, default values are adopted.

2.2.3 Wired-to-Wireless Priority Mapping

Scenario

Figure 2-4 Wired-to-wireless packet priority mapping



PC-to-station QoS mapping process:

- The AC receives an 802.3Mac packet from the PC.

- Set the internal COS priority of the packet based on the trust mode of the physical port. If the trusted packet has the 802.1p priority and carries tag, set the internal COS priority of the packet based on the 802.1p priority. Otherwise, set the default priority of the packet based on the default priority of the port. If the trust mode is DSCP priority, the preceding setting shall be performed based on the DSCP priority of the incoming wireless packet. Currently, the default ETH trust mode is DSCP, and the wireless end always maps to the dot11e.
- The AC encapsulates the 802.3 packet into a CAPWAP packet.
- After receiving the CAPWAP packet, the AP decapsulates the packet and performs QoS priority mapping for the wired-to-wireless packet generated after decapsulation based on the trust mode of QoS priority. If the trust mode is DSCP, the AP configures 802.11e and DSCP filed of the wireless packet based on the DSCP field value of the 802.3 packet. If the trust mode is 802.1p, the AP performs relevant settings based on the COS field of the 802.3 packet.
- Based on the 802.11e priority of the wireless packet, the AP participates in the competition for wireless channels and sends the wireless packet to the STA.

Deployment

The device should be configured with the following key points:

- Enable the WMM.
- Set the wired-to-wireless priority mapping table. Generally, default values are adopted.

2.3 Features

Basic Concepts

Access Class

According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. From the lowest priority to the highest priority, the sequence is as follows: AC_BK, Background <AC_BE, Best Efforts<AC_VI, Video Data <AC_VO, Voice Data.

EDCA Competitive Mechanism

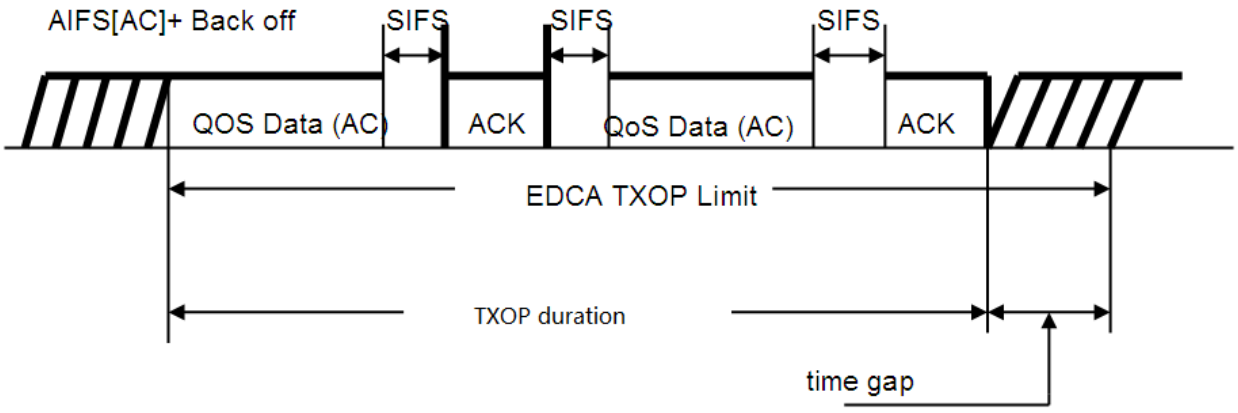
The EDCA competitive mechanism is the core of the IEEE 802.11e. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities. Enhanced distributed channel access (EDCA) not only retains distributed channel competition between the AP and STA, but also introduces internal competition of four internal priority classes of QAP/QSTA. In this way, EDCA introduces the channel competition mechanism for differentiating the priority classes between different QAPs and QSTAs through the wireless air interface. Competition for channels is implemented by configuring EDCA competition parameters of different priority classes. The QAP pushes the configuration to the QSTA and controls the access capability of the QSTA. Competition parameters include AIFS, TXOP Limit, CWmin, and CWmax.

EDCA Parameters

The EDCA competition parameters are listed as follows:

- AIFSN (Arbitration Inter Frame Spacing Number): In the 802.11 protocol, the Distributed Inter-frame Spacing (DIFS) is a fixed value. However, the DIFS for different ACs of the WMM can be set to different values. A larger AIFSN value means a longer DIFS. A shorter DIFS means a bigger probability of preempting channels.
- ECWmin (Exponent form of CWmin) and ECWmax (Exponent form of CWmax) determine the average backoff time. Larger ECWmin and ECWmax mean a longer backoff time.
- TXOP (Transmission Opportunity): maximum duration for preempting channels after successful competition by a user at one time. A larger TXOP means a longer duration for a user to preempt channels. If the TXOP value is 0, only one packet is sent after channel preemption each time. If a frame is too large to be completely sent within the TXOP, this frame must be segmented.

Figure 2-5 TXOP successive frame transmission



ACK Policy

Two ACK policies are available, that is, Normal ACK and No ACK.

- Normal ACK: After receiving a unicast packet successfully, the recipient returns an ACK response.
- No ACK: In the environment with high communication quality and little interference, you can configure the mechanism of not returning an ACK packet for the flow of a certain priority for confirmation, saving the channel resource. During wireless packet interaction, it is not necessary that an ACK packet is used for confirmation. The No ACK policy helps to improve the transmission efficiency effectively. However, it may cause packet loss.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

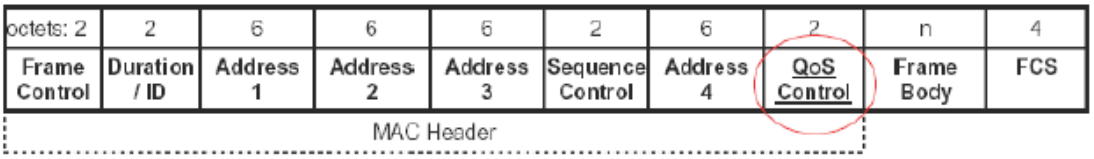
AC Queue Depth

If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

802.11e Priority

802.11e extends the MAC header of 802.11, with the QoS Control domain added, as shown in Figure 2-6.

Figure 2-6 802.11e MAC Header



The QoS Control domain has two bytes. Among them, the first three bits are the TID field, indicating the data form identification code. TID values 0-7 are used for QoS with priorities, indicating the priorities (UP) of users; TID values 8-15 are used for parameter-based QoS, indicating the data flow ID (TSID).

The WMM maps UP to corresponding AC. The following table lists the mapping between the 802.11e priority and AC.

Priority	UP (User Priority)	AC (Access Category)
Lowest ↓ **Highest**	1	Back-ground
	2	Back-ground
	0	Best-effort
	3	Best-effort
	4	Video
	5	Video
	6	Voice
	7	Voice

↘ Priority Mapping Table

After a packet enters a device, the device judges the packet trust mode of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (fat AP or fit AP) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

Overview

Feature	Description
WMM Service	Configure WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.
QoS Packet Priority Mapping	Configure QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

2.3.1 WMM Service

Configure WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.

Working Principle

Provide network services of different quality based on various requirements. That is, provide high-quality services for key data packets having high timeliness requirement and process them preferentially, and assign a low processing priority to

common packets not having high timeliness requirement. According to the WMM standard, access data flows have four priorities. Each priority can be regarded as a class. The EDCA differentiates the access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities.

Enabling WMM

Enable/disable the WMM service. When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

EDCA Competitive Mechanism, AC Queue Depth, and NO ACK Policy

- EDCA competitive mechanism:

EDCA parameters differentiate the channel access capabilities of different priorities. Each AC has its own EDCA channel competition parameters. Users can adjust the values of the EDCA parameters on the client or AP based on actual requirements to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel. The channel competition should be completed automatically by the hardware. The hardware would be engaged in the channel competition after parameters such as CWmin, CWmax, AIFSN, TXOP of each hardware queue are set on the software.

During actual configuration, you can choose to configure the EDCA parameters on the client side or AP side based on application requirements. The configuration of edca-client mainly affects the wmm competition parameters of sta, and the configuration of edca-radio mainly affects the wmm competition parameters of AP.

The QSTA configuration is managed and pushed by the QAP in a centralized manner. The channel competition parameters of QAP and QSTA are mutually independent. Generally, the channel competition parameters of QAP would be slightly increased to ensure competent channel control capability for QAP. QAP would notify the EDCA parameter setting of QAP through the EDCA Parameter Set IE of the frame of beacon or Probe Response, and push the negotiated EDCA configuration to QSTA through EDCA Parameter Set IE of the (Re)Association Response frame.

- AC queue depth:

Set the AC queue depth. If the queue depth of packets of a certain priority is greater than the preset AC queue depth, subsequent packets are discarded. Otherwise, subsequent packets are added to the queue for processing according to normal logics.

- NO ACK policy:

Enable/disable the NO ACK (No Acknowledgement) policy. The NO ACK policy should be supported by the recipient and the sender at the same time. When the NO ACK policy frame transmission chip does not support NO ACK policy for a queue, the NO ACK policy should be set in the DMA descriptor of each frame sent at each frame sent.

The NO ACK policy is used as an alternative for the method of receiving confirmation (during wireless packet exchange) by using ACK packets in the environment with high communication quality and little interference. The NO ACK policy helps to effectively improve the transmission efficiency. However, if ACK packet for confirmation is not used and the communication quality is poor, the sender would not retransmit the packets even if the recipient has not received the packets, resulting in increasing packet loss rate.

2.3.2 QoS Packet Priority Mapping

Configure QoS packet priority mapping, including the QoS packet priority mapping table and priority mapping policy.

Working Principle

The priority mapping tables provided by the device correspond to relevant priority mapping respectively. Then, a mapping table is selected based on the preset information to perform the priority mapping operation, thereby implementing end-to-end QoS for the entire network.

Packet Priority Mapping

In the IP network, IPv4 packets carry QoS priority tags in three modes, that is, layer 2-based CoS field (IEEE802.1p) priority, IP layer-based IP priority field ToS priority, and IP layer-based DSCP (Differentiated Services Codepoint) field priority.

For the three QoS priority tags of wired packets, it is sufficient to support the two kinds of QoS (DSCP and dot1P) because DSCP is compatible with ToS. In addition to the preceding three modes, the QoS priority tag mode of dot11e is also available for wireless packets.

As for the determination and execution of packet priority mapping, the device judges the packet trust mode or tag policy of the current interface, that is, judges which part of priority information in the received packet is valid. In addition, the device judges the work mode (centralized forwarding or local forwarding) of the current AP. Then, the device selects a mapping table based on the preset information to perform the priority mapping operation.

2.4 Configuration

Configuration	Description and Command	
Configuring the WMM Service	(Mandatory). It is used to enable the WMM service.	
	wmm enable	Enables the WMM service.
	(Optional). It is used to configure competition parameters.	
	wmm edca-client	Configures the EDCA parameters for the client.
	wmm edca-radio	Configures the EDCA parameters for the AP.
Configuring the QoS Packet Priority Mapping	(Optional). It is used to configure the priority mapping. Mapping command for non-interworking versions.	
	wlan-qos map-table	Configures packet priority mapping of the current WLAN.
	(Optional). It is used to configure the 802.11p QoS mapping policy mechanism. Mapping command for interworking versions.	

Configuration	Description and Command	
	wmm dot1p enable	Enables 802.11p QoS mapping policy mechanism.
	wmm dot1p policy 1q	Configures how to apply the 802.11p QoS mapping policy mechanism for the AP.
	wmm dot1p tag	Configures 802.1p priority.
	(Optional) . It is used to configure the DSCP QoS mapping policy mechanism. Mapping command for interworking versions.	
	wmm dscp enable	Enables DSCP QoS mapping policy mechanism.
	wmm dscp policy **outer-tunnel** **inner-tunnel**	Configures how to apply the DSCP QoS mapping policy mechanism for the AP.
	wmm dscp tag	Configures DSCP identifications.

2.4.1 Configuring the WMM Service

Configuration Effect

- Configure the EDCA competition parameters for the client.
- Configure the EDCA competition parameters for the AP.
- Configure the ACK policy.
- Configure the length of the priority queue.

Notes

- The parameter configuration takes effect after the WMM service is enabled.
- When the WMM service is enabled and the BE queue adopts the default configuration, the Xspeed function dynamically adjusts the parameters of the BE queue.

Configuration Steps

Enabling the WMM Service

- Mandatory configuration.
- Run the **wmm enable radio** *radio-id* command in AP configuration mode to enable the WMM for the fit AP.
- When the WMM service is enabled, the four-level priority queue is used for reception and mapping. When the WMM service is disabled, the default priority queue is used for reception and mapping.

Command	**wmm enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled WMM service is selected. Value range: 1-48.

Defaults	WMM is enabled by default
Command Mode	AP configuration mode
Usage Guide	When the WMM service is disabled, the default priority queue is used for reception and mapping.

Configuring the EDCA Parameters for the Client

- Optional configuration.
- By default, the EDCA parameters on the client side are as follows:

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

- After the EDCA parameters on the client side and AC queue depth are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **length** [*queue-length*] } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: Sets the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: Sets the cwmax value. Value range: 0-15. **txop** *txop-value*: Sets the txop value. Value range: 0-255, unit: 32 μs. **length** *queue-length*: Sets the AC queue length. Value range: 1-255. The default is 255. **radio** *radio-id*: Sets radio of the EDCA parameters on the client. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Configuring the EDCA Parameters for the AP

- Optional configuration.
- By default, the EDCA parameters on the AP side are as follows:

AC	aifs	cwmin	cwmax	txop

back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

- After the EDCA parameters on the AP side and NO ACK policy are set to non-default settings, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.
- Smaller AIFS of a high-priority AC means earlier backoff process. Smaller CWmin and CWmax values mean shorter backoff time. TXOP limit allows an AC to transmit multi-frame packets on it continuously within the SIFS interval after preempting a transmission opportunity. A larger TXOP limit means a lower packet conflict rate and a lower waste of air interface resources.

Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin** [*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the aifsn value. Value range: 1-15. **cwmin** *cwmin-value*: Sets the cwmin value. Value range: 0-15. **cwmax** *cwmax-value*: Sets the cwmax value. Value range: 0-15. **txop** *txop-value*: Sets the txop value. Value range: 0-255, unit: 32 μs. **noack**: Indicates that the no ack policy is enabled. The no ack policy is disabled by default. **radio** *radio-id*: Sets radio of the EDCA parameters on the client. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The cwmax value must be greater than the cwmin value. Otherwise, a configuration error message is displayed.

Verification

- You can run the **show run/show ap-config run** command on the fit AP to display the WMM service status. The EDCA parameters of the client that already take effect and the EDCA parameters used for the AP are not displayed when they adopt default settings.
- Capture packets to display the EDCA parameters of the client.

Configuration Example

Configuring WMM Service Parameters

Configuration Steps	• Enable/disable the WMM service on the AP. • Configure the EDCA parameters for the client.

	• Configure the EDCA parameters for the AP.
	Ruijie # configure terminal Ruijie(config)# ap-config AP001 Ruijie(config-ap)# wmm enable radio 1 Ruijie(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1 Ruijie(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
Verification	Run the **show run**/**show ap-config run** command on the fit AP to display the EDCA parameters of the client that already take effect and the EDCA parameters used for the AP. These parameters are not displayed when they adopt default settings.

Common Errors

- If no radio exists, an error message is displayed.
- The performance is affected if EDCA parameters are improperly configured. For example, if the value of a low-priority parameter is higher than that of a high-priority parameter, the performance of the high priority is affected.

2.4.2 Configuring the QoS Packet Priority Mapping

Configuration Effect

- Configure packet priority mapping for the current WLAN.
- Configure 802.11p QoS mapping policy mechanism.
- Configure DSCP QoS mapping policy mechanism.

Notes

- QoS packet priority mapping takes effect after the WMM service is enabled.

Configuration Steps

By default, the mapping from DSCP to 802.11e is as follows:

DSCP	802.11e
0-7	0
16-23	1
24-31	2
8-15	3
32-39	4
40-47	5
48-55	6
56-63	7

By default, the mapping from 802.11e to DSCP is as follows:

802.11e	DSCP
0	0
3	8
1	16
2	24
4	32
5	40
6	48
7	56

Configuring Packet Priority Mapping for the Current WLAN

- Optional configuration.
- Unless otherwise specified, packet priority mapping of the current WLAN shall be configured on all APs.

After the priority mapping and the value corresponding to the mapping table are set, relevant processing is conducted based on the settings. Otherwise, processing is conducted based on the default settings.

Command	**wlan-qos map-table** { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*
Parameter Description	**dot11e-inner-dscp**: Sets priority mapping from dot11e to internal DSCP. **dot11e-tunnel-dscp**: Sets priority mapping from dot11e to CAPWAP DSCP. **dscp-dot11e**: Sets priority mapping from dscp to dot11e. **import** *import-tag-value*: Sets priority of the incoming original packet. **export** *export-tag-value*: Sets priority of the outgoing packet. **no**: Restores the default setting.
Command Mode	WLAN configuration mode
Usage Guide	This command is a mapping command for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled.

Enabling 802.11p QoS Mapping Policy Mechanism

- Optional configuration.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the 802.11p QoS policy mechanism is enabled, the mapping table related to 802.11p QoS is used. When the 802.11p QoS policy mechanism is disabled, the default mapping policy is adopted.

Command	**wmm dot1p enable radio** *radio-id*
Parameter	**radio** *radio-id*: Indicates that radio of the enabled/disabled 802.11p QoS mapping policy mechanism is

Description	selected. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the 802.11p QoS Mapping Policy Mechanism for the AP

- Optional configuration.
- Unless otherwise specified, the 802.11p QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the 802.1Q priority be obtained based on the configuration determining how the AP applies the 802.11p QoS mapping policy mechanism.

Command	**wmm dot1p policy 1q** [*1q-policy-value*] **radio** *radio-id*
Parameter Description	**1q** *1q-policy-value*: Indicates setting for applying the 802.11p QoS mapping policy mechanism. Value range: 0-1. The default is **0**. **radio** *radio-id*: Indicates how the AP applies radio of 802.11p QoS mapping policy mechanism. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the 802.11p QoS mapping policy mechanism takes effect only when the 802.11p QoS mechanism is enabled.

Configuring 802.1p Priority

- Optional configuration.
- Unless otherwise specified, 802.1p priority shall be configured on all APs.

Determine the priority of 802.1p based on the configuration of 802.1p priority.

Command	**wmm dot1p tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the 802.1p priority. Value range: 0-7. The default **best-effort** is **0**; the default ;**back-ground** is **2**; the default **video** is **4**; the default **voice** is **6**. **back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Indicates that radio of the enabled/disabled 802.11p QoS mapping policy mechanism is selected. Value range: 1-96. **no**: Restores the default settings.
Command	AP configuration mode

Mode	
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The 802.1p priority configuration takes effect only when the 802.11p QoS mechanism is enabled.

Enabling DSCP QoS Mapping Policy Mechanism

- Optional configuration.
- Unless otherwise specified, DSCP QoS mapping policy mechanism shall be disabled on all APs.

When the DSCP QoS policy mechanism is enabled, the mapping table related to DSCP QoS is used. When the DSCP QoS policy mechanism is disabled, the default mode is adopted for mapping.

Command	**wmm dscp enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled DSCP QoS mapping policy mechanism is selected. Value range: 1-96. **no**: Restores the default settings.
Defaults	
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Configuring How to Apply the DSCP QoS Mapping Policy Mechanism for the AP

- Optional configuration.
- Unless otherwise specified, the DSCP QoS mapping policy mechanism application shall be performed on all APs.

Determine where shall the DSCP domain priority be obtained based on the configuration determining how the AP applies the DSCP QoS mapping policy mechanism.

Command	**wmm dscp policy outer-tunnel** [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*
Parameter Description	**outer-tunnel** *outer-tunnel-value*: Sets how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header. Value range: 0-1. The default is **0**. **Inner-tunnel** *inner-tunnel-value*: Sets how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header. Value range: 0-1. The default is **0**. **radio** *radio-id*: Indicates how the AP applies radio of DSCP QoS mapping policy mechanism. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The configuration for applying the DSCP QoS mapping policy mechanism takes effect only when the DSCP QoS mechanism is enabled.

Configuring DSCP Identification

- Optional configuration.
- Unless otherwise specified, DSCP identifications shall be configured on all APs.

Determine the DSCP priority based on the configured DSCP identifications.

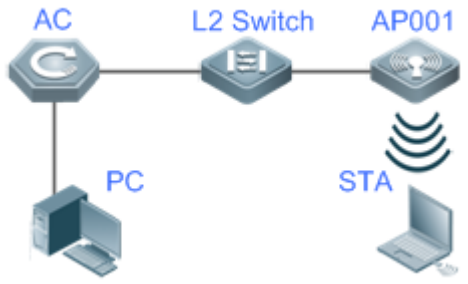
Command	**wmm dscp tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the DSCP priority. Value range: 0-63. The default **best-effort** is **0**; the default **back-ground** is **16**; the default **video** is **32**; the default **voice** is **48**. **back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Sets radio of the DSCP identifications. Value range: 1-96. **no**: Restores the default settings.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. DSCP identification configuration takes effect only when the DSCP mechanism is enabled.

Verification

- You can run the **show run**/**show ap-config run** command on the fit AP to display the mapping configuration information. When the default configuration is adopted, no configuration information is displayed in the command output.
- Capture packets to check whether the priority mapping is correct.

Configuration Example

Configuring the QoS Packet Priority Mapping

Scenario	
	Connect the AC to the L2 switch, and connect AP001 to the AC through the L2 switch. Configure WLAN1 on AP001. Connect STA to AP001 in wireless mode, and connect the PC to the AC in wired mode.

Configuration Steps	Perform the following configuration on the AC: ● Enter the specified WLAN configuration mode. ● Configure the packet priority mapping.
	Ruijie# configure terminal Ruijie(config)# wlan-config 1 Ruijie(config-wlan)#wlan-qos map-table dot11e-tunnel-dscp import 7 export 50 Ruijie(config-wlan)# end
Verification	Import AC_VO priority traffic in the direction from the STA to PC by using IxChariot, capture packets on the air interface, and display the priority at the wireless end. Then, capture packets from the AC to PC using a packet capturing tool to display the priority at the wired end.

Common Errors

- The WMM service is disabled.

2.5 Monitoring

Debugging

⚠ Outputting debugging information consumes system resources. Disable the debugging function immediately after using it.

Command	Function
debug wlan-qos-vsp	Debugs WMM VSP.
debug wlan-qos-cli	Debugs WMM CLI.
debug wlan-qos-map	Debugs WMM mapping.

3 Configuring VIP-FIRST

3.1 Overview

VIP-FIRST is a function used to improve the wireless user experience, which covers preferred access and independent rate limiting for VIP users.

Preferred access for VIP users ensures that VIP users can access the network at any time without being affected by the STA-LIMIT function.

Independent rate limiting for VIP users indicates that an independent rate limit can be configured for VIP users to prevent them being affected by the global rate limit.

3.2 Applications

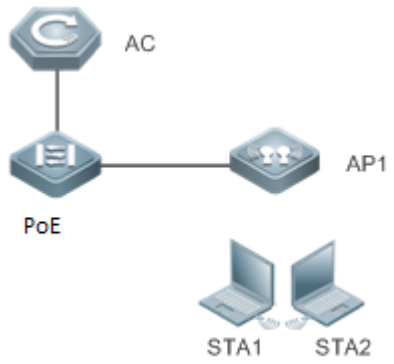
Application	Description
VIP-FIRST in fit AP networking	Fit AP networking is adopted, including at least one AC and one AP.

3.2.1 VIP-FIRST in Fit AP Networking

Scenarios

On the wireless network, an AC is deployed with preferred access and independent rate limit enabled for VIP users. The VIP user list is uploaded to a specific directory on the AC, and the **import** command is run to advertise for the AC to parse the VIP user list, as shown in the following figure.

Figure 3-1



Remarks	AC: wireless access controller PoE: switch, used as the gateway of the AP. AP: wireless access point STA1 and STA2: wireless stations

Deployment

- Enable the VIP-FIRST function on the AC.

3.3 Features

Basic Concepts

Preferred Access for VIP Users

When there are a large number of STAs, the network experience of some STAs may be affected. If the number of STAs connected to the AC, WLAN, AP, or radio exceeds the limit specified by the STA-LIMIT function, preferred access for VIP users ensures that a non-VIP user with poor communication quality is kicked off to ensure that a VIP user can access the network.

Independent Rate Limiting for VIP Users

When there are a large number of STAs, the network experience of some users may be affected. In addition to the global rate limit, an independent rate limit is configured for VIP users to ensure that the bandwidth of VIP users is higher than that of common users.

Overview

Feature	Description
Preferred Access for VIP Users	Ensures that VIP users can access the network at anytime.
Independent Rate Limiting for VIP Users	Ensures that the bandwidth of VIP users is higher than that of common users.

3.3.1 Preferred Access for VIP Users

Preferred access for VIP users ensures that VIP users can access the network anytime without being affected by the STA-LIMIT function.

Working Principle

If the number of STAs connected to the AC, WLAN, AP, or radio exceeds the limit specified by the STA-LIMIT function, a non-VIP user with poor communication quality will be kicked offline to ensure that a VIP user can access the network.

3.3.2 Independent Rate Limiting for VIP Users

In addition to the global rate limit, an independent rate limit is configured for VIP users to ensure that the bandwidth of VIP users is higher than that of common users.

Working Principle

When the global rate limit is configured, a higher independent rate limit is configured for VIP users.

3.4 Configuration

Configuration	Description and Command	
Configuring VIP user parsing or deletion	(Mandatory) It is used to advertise for the AC to parse the VIP user list.	
	vip-first import	Advertises for the AC to parse the VIP user list.
	(Optional) It is used to advertise for the AC to delete the VIP user list.	
	vip-first clear	Clears the VIP user list from the AC.
Configuring Preferred Access for VIP Users	(Mandatory) It is used to enable preferred access for VIP users.	
	vip-first prior-assoc	Enables preferred access for VIP users on the AC.
Configuring Independent Rate Limiting for VIP Users	(Mandatory) It is used to enable independent rate limiting for VIP users.	
	vip-first rate-limit	Configures the uplink and downlink rate limits for VIP users on the AC.

3.4.1 Configuring VIP User Parsing or Deletion

Configuration Effect

- Advertise for the AC to parse or delete the VIP user list.

Notes

- Upload the VIP user list file to the **flash** directory and then run the **import** command to advertise for the AC to parse the VIP user list. It takes several to dozens of seconds for the AC to parse the VIP user list.
- The VIP user list file is named **vip_user_list.txt**.
- The **clear** command will delete VIP users and the VIP user list file cached on the AC.
- The VIP user parsing or deletion command is not saved.

Configuration Steps

Advertising for the AC to Parse the VIP User List

- Mandatory.
- Run the **vip-first import** command in global configuration mode on the AC.

Command	vip-first import
Parameter	N/A

Description	
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show vip-first user [mac]** command to check whether a user is a VIP user.

Advertising for the AC to Delete the VIP User List

- Optional.
- Run the **vip-first clear** command in global configuration mode on the AC.

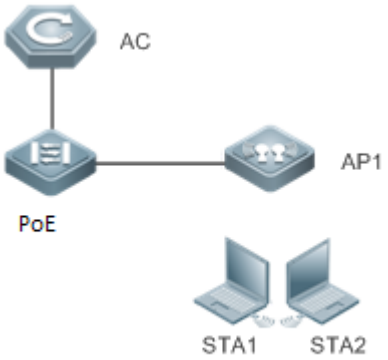
Command	**vip-first clear**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **dir** command to check whether the vip_user_list.txt file exists.

Configuration Example

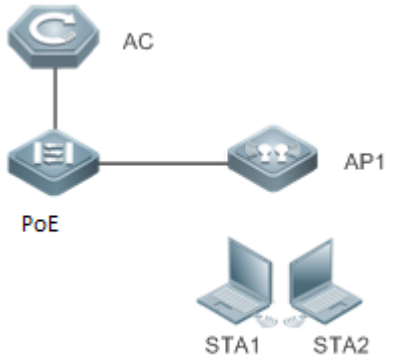
Advertising for the AC to Parse the VIP User List

Scenario Figure 3-2	
Configuration Steps	● Advertise for the AC to parse the VIP user list in global configuration mode.
AC	`Ruijie#configure terminal`

	Ruijie(config)# vip-first import Ruijie(config-ap)# exit
Verification	Run the **show vip-first user [mac]** command to display configuration.
AC	AC_20_3F#show vip-first user 0000.0000.0001 STA_MAC YES/NO ------------ ------ 0000.0000.0001 YES

Configuration Example

Deleting the VIP User List

Scenario Figure 3-3	
Configuration Steps	● Advertise for the AC to delete the VIP user list in global configuration mode.
AC	Ruijie#configure terminal Ruijie(config)# vip-first clear Ruijie(config-ap)# exit
Verification	Check whether the **vip_user_list.txt** file exists in the **flash** directory.
AC	AC_20_3F# dir Number Properties Size Time Name ------ ---------- ------ ------------------------ -------------------- 1 drwx 160B Tue Apr 25 08:39:38 2017 dev 2 drwx 160B Thu Nov 24 18:06:41 2016 rep 3 drwx 224B Thu Nov 24 18:06:42 2016 var

Common Errors

- The **vip-first import** command is run to advertise for the AC to parse the VIP user list before the **vip_user_list.txt** file is uploaded to the AC.

3.4.2 Configuring Preferred Access for VIP Users

Configuration Effect

- Enable VIP users to access the network anytime without being affected by the STA-LIMIT function.

Notes

- The function can be configured only in global configuration mode on the AC.

Configuration Steps

↘ Enabling Preferred Access for VIP Users

- Mandatory.
- Run the **vip-first prior-assoc** command in global configuration mode on the AC.
- Enable preferred access for VIP users to ensure that VIP users can access the network anytime without being affected by the STA-LIMIT function.

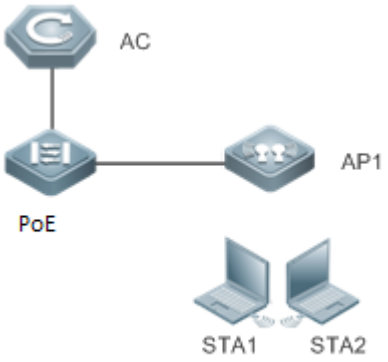
Command	**vip-first prior-assoc**
Parameter Description	N/A
Defaults	Preferred access for VIP users is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to display configuration.

Configuration Example

↘ Enabling Preferred Access for VIP Users

Scenario **Figure 3-4**	
Configuration Steps	● Enable preferred access for VIP users in global configuration mode on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)# vip-first prior-assoc` `Ruijie(config-ap)# exit`
Verification	Run the **show running-config** command to display configuration.
AC	`Ruijie# show ap-config running` `!` `vip-first prior-assoc!`

3.4.3 Configuring Independent Rate Limiting for VIP Users

Configuration Effect

- Ensure that the bandwidth of VIP users is higher than that of common users.

Notes

- An independent rate limit can be configured for VIP users only after a global rate limit is configured, and the VIP user rate limit must be greater than the global rate limit. The global rate limit takes effect to all STAs under the AC.

Configuration Steps

↘ Enabling Independent Rate Limiting for VIP Users

- Mandatory.
- Global configuration mode
- Enable independent rate limiting for VIP users to increase the bandwidth of VIP users.

Command	**vip-first rate-limit** { **down-stream** | **up-stream** } **average-rate** *average-rate* **burst-rate** *burst-rate*
Parameter	**down-streams**: Sets the downlink rate limit of an AP.

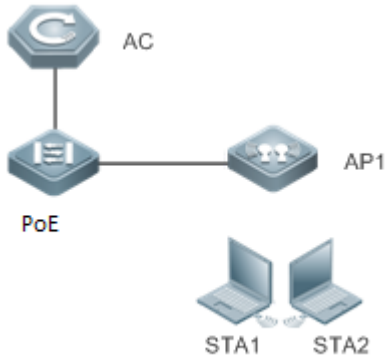
Description	**up-streams**: Sets the uplink rate limit of an AP. *average-rate*: Sets the average rate limit by a step of 8 kbit/s. The value range is **8** to **261120**. *burst-rate*: Sets the burst rate limit by a step of 8 kbit/s. The value range is **8** to **261120**.
Defaults	Independent rate limiting for VIP users is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to display configuration.

Configuration Example

Enabling Independent Rate Limiting for VIP Users

Scenario Figure 3-5	
Configuration Steps	● Enable independent rate limiting for VIP users in global configuration mode on the AC.
AC	`Ruijie#configure terminal` `Ruijie(config)# vip-first rate-limit up-stream average-rate 8 burst-rate 8` `Ruijie(config)# vip-first rate-limit down-stream average-rate 8 burst-rate 8` `Ruijie(config-ap)#end`
Verification	Run the **show ap-config running** command to display configuration.
AC	`Ruijie# showap-config running` `!` `vip-first rate-limit up-stream average-rate 8 burst-rate 8` `vip-first rate-limit down-stream average-rate 8 burst-rate 8` `!`

3.5 Monitoring

Displaying

Description	Command
Checks whether a user is a VIP user.	**show vip-first user [mac]**

WLAN Networking Configuration

1. Configuring WLAN Hot Backup
2. Configuring WDS
3. Configuring RIPT
4. Configuring Virtual AC
5. Configuring Bonjour Gateway

1 Configuring WLAN Hot Backup

1.1 Overview

Wireless LAN (LAN) hot backup is a wireless dual-host hot backup function.

The WLAN hot backup function enables switchover of the Control and Provisioning of Wireless Access Points (CAPWAP) tunnels between access controllers (ACs) and access points (APs) within several milliseconds when an AC is unreachable or faulty, thus ensuring uninterrupted services for associated stations (STAs) to the maximum extent.

Working modes of WLAN hot backup include the Active/Standby (A/S) mode and the Active/Active (A/A) mode.

WLAN hot backup is applicable to a reliability-sensitive wireless network.

Protocols and Standards

- N/A

1.2 Applications

Application	Description
1+1 A/S Networking	Two ACs are deployed. AC-1 and AC-2 are configured as hot backup ACs working in A/S mode.
1+1 A/A Networking	Two ACs are deployed. AC-1 and AC-2 are configured as hot backup ACs working in A/A mode.
N+1 A/S Networking	N+1 ACs are deployed and configured as hot backup ACs working in A/S mode.
Hierarchical AC Networking	A special N+1 networking mode, which is adopted in hierarchical AC scenarios.

1.2.1 1+1 A/S Networking

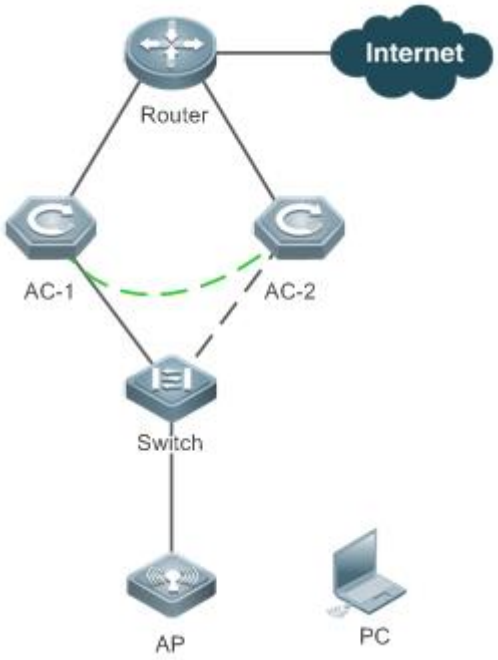
Scenario

On a wireless network, two ACs are deployed. One AC works as the active AC and provides services to external entities. The other AC works as the standby AC and receives data synchronized from the active AC.

When the active AC is unreachable due to some reasons (for example, because the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the standby AC can take over services from the active AC to ensure that the wireless network is not affected.

As shown in Figure 1-1, when AC-1 is unreachable but the switch and other devices work normally, AC-2 takes over services from AC-1. The wireless network is not affected and can still provide wireless services normally.

Figure 1-1



Remarks	Router is a routing device that functions as the gateway of STAs. AC-1 and AC-2 are wireless access controllers. Switch is a convergence device that functions as the gateway of APs. AP is a wireless access device. PC is a user device that functions as a STA.

Deployment

- Enable the WLAN hot backup function on AC-1 and AC-2, and configure a hot backup context.
- Add the AP group to which the AP belongs to the WLAN hot backup context.

1.2.2 1+1 A/A Networking

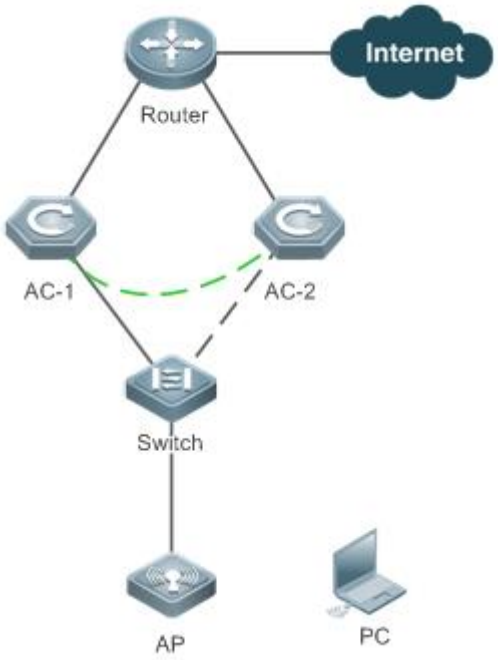
Scenario

On a wireless network, two ACs are deployed. Both ACs work as the active ACs and provide services to external entities. Both ACs work as the standby AC of the peer AC and receive data synchronized from the peer AC.

When one AC is unreachable due to some reasons (for example, because the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the other AC can take over services from the unreachable AC to ensure that the wireless network is not affected.

As shown in Figure 1-2, when AC-1 is unreachable but the switch and other devices work normally, AC-2 takes over services from AC-1. The wireless network is not affected and can still provide wireless services normally.

Figure 1-2



Remarks	Router is a routing device that functions as the gateway of STAs. AC-1 and AC-2 are wireless access controllers. Switch is a convergence device that functions as the gateway of APs. AP is a wireless access device. PC is a user device that functions as a STA.

Deployment

- Enable the WLAN hot backup function on AC-1 and AC-2, and configure two hot backup contexts.
- Add the AP group to which the AP belongs evenly to the two WLAN hot backup contexts.

1.2.3 N+1 A/S Networking

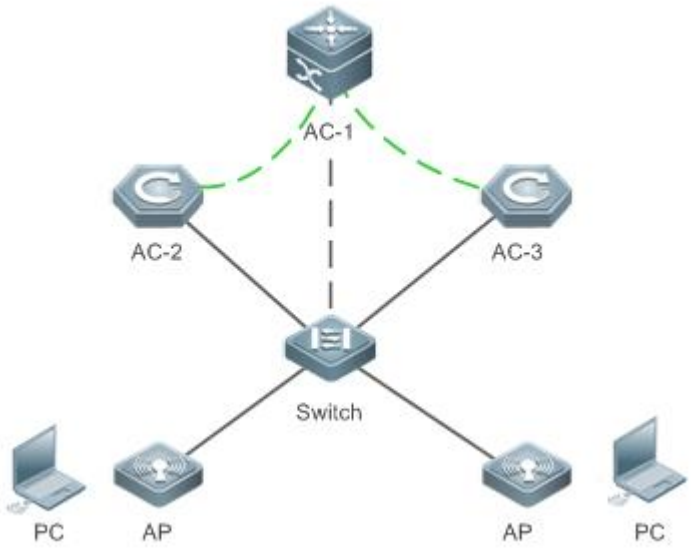
Scenario

On the wireless network, N+1 ACs are deployed. *N* ACs work as the active ACs and provide services to external entities. The other AC works as the standby AC and receives data synchronized from the active ACs.

When one active AC is unreachable (for example, when the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the standby AC can take over services from the active AC to ensure that the wireless network is not affected.

As shown in Figure 1-3, when AC-2 is unreachable but the switch, APs, and other devices work normally, AC-1 takes over services from AC-2. The wireless network is not affected and can still provide wireless services normally.

Figure 1-3



Remarks	Router is a routing device that functions as the gateway of STAs. AC-1, AC-2, and AC-3 are the wireless access controllers. Switch is a convergence device that functions as the gateway of APs. AP is a wireless access device. PC is a user device that functions as a STA.

The N+1 A/S networking mode is not compatible with the 1+1 A/A networking mode.

Deployment

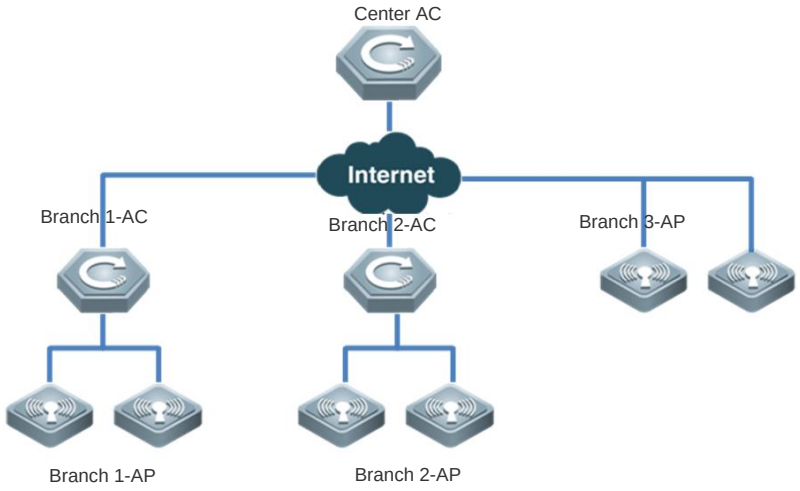
- Enable the WLAN hot backup function on AC-1, and configure two hot backup contexts. Enable the WLAN hot backup function on AC-2 and AC-3, and configure a hot backup context respectively on AC-2 and AC-3.
- Add the AP group to which the AP belongs to the WLAN hot backup context.

1.2.4 Hierarchical AC Networking

Scenario

Hierarchical AC is a centralized management and distributed forwarding model. In this model, ACs are classified into the center AC and branch ACs. A high-performance AC is deployed at the center, and low-end ACs are deployed at braches. The following figure shows the model.

Figure 1-1



Deployment

- Enable the WLAN hot backup function and configure two hot backup instances on the center AC. Enable the WLAN hot backup function and configure one hot backup instance on Branch 1-AC and Branch 2-AC.
- Configure hierarchical AC roles on the center AC, Branch-1 AC, and Branch-2 AC.
- Add the AP groups to which the APs belong to the corresponding WLAN hot backup instances.

1.3 Features

Basic Concepts

AC Keepalive Channel

After the hot backup function is enabled, the active AC periodically sends a keepalive packet to the standby AC, and the standby AC determines whether the active AC works normally based on the received keepalive packet. If the standby AC does not receive the packet in5 consecutive keepalive periods, the standby AC determines that the active AC is faulty, and then notifies APs to activate the standby CAPWAP tunnels.

The keepalive period between ACs is 10s by default and is configurable.

Active CAPWAP Tunnel

To support the hot backup function, an AP must set up CAPWAP tunnels with two ACs that are configured with the hot backup relationship. The CAPWAP tunnel between the AP and the active AC is activated, and is called active CAPWAP tunnel.

Standby CAPWAP Tunnel

The CAPWAP tunnel between an AP and the standby AC is called standby CAPWAP tunnel. The standby CAPWAP tunnel is not used for communication between the AP and the AC.

Hot Backup Context

In A/A mode, the role taken by the same AC varies according to APs. An AC that sets up an active CAPWAP tunnel with an AP serves as the active AC of the AP. An AC that sets up an standby CAPWAP tunnel with an AP serves as the standby AC of the AP. The AC must perform different backup operations when taking different roles. Therefore, on the same AC, different hot backup contexts must be configured so that the AC can perform different backup operations.

Overview

Feature	Description
Configuring the Hot Backup Function	Enable the hot backup function to synchronize the data.

1.3.1 Configuring Hot Backup

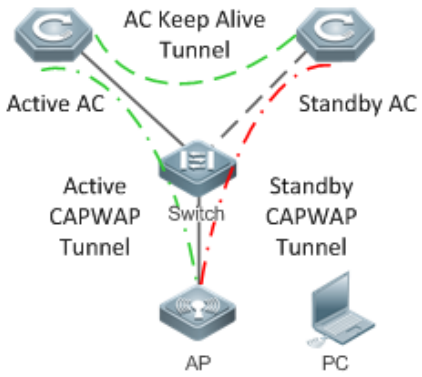
Configure the addresses of hot backup neighbors and contexts, and bind the AP groups, DHCP address pool, and VRRP groups with the corresponding contexts so that the hot backup function is enabled on the AP groups, DHCP address pool, and VRRP groups to support data synchronization and switchover.

Working Principle

The WLAN hot backup detection packet is a UDP packet, and the port ID is 7425. The control channel packet is a TCP packet, and the port ID is 6435. The data channel packet is a TCP packet, and the port ID is 6425. The heartbeat keepalive packet is an IP packet by default and can be configured as the UDP packet, the protocol field is 0, and the port ID is 7435.

WLAN hot backup enables switchover of the CAPWAP tunnels between ACs and APs within several milliseconds when an AC is unreachable or faulty, thus ensuring uninterrupted services for associated STAs to the maximum extent. Figure 1-4 shows the working principle of the WLAN hot backup function.

Figure 1-4 WLAN hot backup



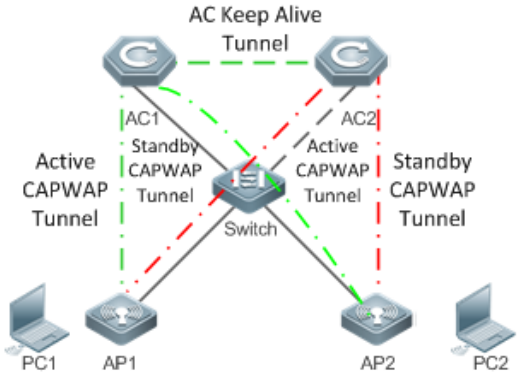
- Two ACs determine the active and standby ACs through negotiation, and the keepalive mechanism is used between ACs.
- The AP sets up an active CAPWAP tunnel with the active AC, and a standby CAPWAP tunnel with the standby AC.

- The user uses a wireless client to associate with the AP.
- The user communicates with entities on the network through the active CAPWAP tunnel.
- When the active AC is faulty, the standby AC detects the keepalive timeout event, and immediately notifies the AP.
- The standby CAPWAP tunnel is activated, and the standby AC becomes the active AC.
- The user's services are recovered after the standby CAPWAP tunnel is activated.
- When the original active AC is recovered, it sets up a hot backup relationship with the new active AC again. Then, the original active AC becomes the standby AC and sets up a standby CAPWAP tunnel with the AP. In this way, the user's services are not interrupted.

Working modes of WLAN hot backup include the A/S mode and the A/A mode.

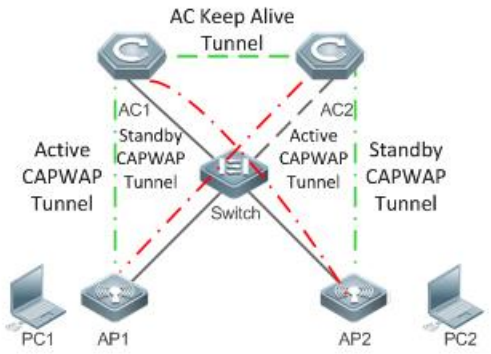
In A/S mode, one AC is the active AC, and the other AC is the standby AC. The active AC processes all services and transfers the service status information to the standby AC for backup purpose. The standby AC does not process services, and only backs up the service data. In A/S mode, all the APs set up active CAPWAP tunnels with the active AC, and standby CAPWAP tunnels with the standby AC. When both ACs work normally, all services are processed by the active AC. When the active AC is faulty, the standby AC takes over all services.

Figure 1-5 WLAN hot backup in A/S mode



In A/A mode, both ACs are active ACs and process services, and meanwhile serve as the standby AC of the other AC and back up the service status information of the other AC. Assume that the two ACs are AC1 and AC2. In A/A mode, some APs set up active CAPWAP tunnels with AC1, and standby CAPWAP tunnels with AC2. Other APs set up active CAPWAP tunnels with AC2, and standby CAPWAP tunnels with AC1. When both ACs work normally, the two ACs process services of APs with which active CAPWAP tunnels are set up. When AC1 is faulty, APs that set up active CAPWAP tunnels with AC1 switch over services to standby CAPWAP tunnels, and then AC2 processes services of all APs.

Figure 1-6 WLAN hot backup in A/A mode



1.3.2 Configuring Hierarchical AC

Working Principle

Hierarchical AC is a special N+1 networking mode. In normal cases, the center AC is a high-performance AC and deployed at the center and branch ACs are deployed at branches. Hierarchical AC ensures unified upgrade, disaster recovery, unified management, and license sharing.

In hierarchical AC scenarios, a new work mode, cold is added, which indicates lightweight data backup. In cold mode, most data backup with the peer is forbidden and only little data transmission is reserved. When traffic of the center AC is heavy, configure the work mode as cold to reduce the load of the center AC. In cold mode, when a branch AC is faulty, STAs need to be re-associated and STAs' IP addresses need to be obtained again for authentication. In cold mode, the unified upgrade, unified management, and license sharing functions are reserved.

1.4 Configuration

Configuration	Description and Command	
Configuring Hot Backup	(Mandatory) It is used to enable the hot backup function.	
	wlan hot-backup	Configures a hot backup neighbor.
	context	Configures a hot backup context.
	wlan hot-backup enable	Enables the hot backup function.
	(Optional) It is used to adjust the hot backup connection parameters.	
	local-ip	Configures the IP address of the local AC for the hot backup function.
	work-mode	Configures the hot backup working mode.
	hello-interval	Configures the heartbeat keepalive period for the hot backup function.

	kplv-pkt	Configures the format of the heartbeat keepalive packet for hot backup.
	priority level	Configures the priorities of contexts.
	ap-group	Binds an AP group with a context.
	dhcp-pool	Binds a DHCP address pool with a context.
	dhcpv6-pool	Binds a DHCPv6 address pool with a context.
	vrrp interface group	Binds a VRRP group with a context.
	description	Describes the hot backup peer.
Configuring Hierarchical AC	⚠ (Mandatory) It is used to enable the hierarchical AC function.	
	wlan hot-backup [center | branch]	**wlan hot-backup [center | branch]**
	⚠ (Optional) It is used to set the lightweight backup mode.	
	work-mode cold	**work-mode cold**

1.4.1 Configuring the Hot Backup Function

Configuration Effect

- Configure a hot backup connection to provide the hot backup service for other modules.

Notes

- After the hot backup function is enabled, the hot backup related configurations cannot be modified.

Configuration Steps

↘ Configuring the Basic Information about Hot Backup

- (Mandatory) The configuration is performed on the AC.
- Run the **wlan hot-backup** command to configure a hot backup neighbor. Unless otherwise specified, you must configure a hot backup neighbor on both ACs. Enter the hot backup configuration mode, and configure the working mode and context for the hot backup function.
- In the hot backup configurations, the peer IP address is the loopback IP address of the peer AC. Ensure that the loopback IP address has been correctly configured; otherwise, hot backup may fail. In addition, configure the related routes to ensure that the local and peer loopback IP addresses can be pinged successfully from each other.
- Run the **context** command to configure a context. Unless otherwise specified, you must configure the same context on both ACs.

Command	**wlan hot-backup** *ip-address*
Parameter Description	*ip-address*: indicates the IP address of the peer AC.
Defaults	No hot backup neighbor is configured.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Command	**context** *context-id*
Parameter Description	*context-id*: indicates the ID of the context.
Defaults	N/A
Command Mode	Hot backup configuration mode
Usage Guide	The value range is 0 to 65,535. In hierarchical AC scenarios, the value is 0-0.

Adjusting the Hot Backup Parameters

- (Optional) The configuration is performed on the AC.
- Run the **local-ip** command to configure the IP address of the local AC for hot backup. By default, the IP address of the Loopback 0 interface on the AC is used. You can configure another IP address of the AC for setting up a hot backup relationship with the peer AC.
- Run the **work-mode** command to configure the hot backup working mode. Hot backup is switched to the quick switchover mode only in an environment that requires quick switchover, for example, in the onsite test environment. Two hot backup working modes are available: (1) Quick switchover mode: It is used in performance switchover scenarios that require sensitive detection and quick switchover, such as system demonstration and performance test. The purpose is to realize quick switchover. The default detection period is 10 ms. (2) Normal switchover mode: It is used in real-life application scenarios that require stable running and avoid hot backup flapping. The purpose is to realize normal running of the network. The default detection period is 2s.
- Run the **hello-interval** command to configure the heartbeat keepalive period for the hot backup function. If quick switchover is required, you can set this parameter to a smaller value to increase the speed of hot backup detection and switchover. A smaller value of **hello-interval** indicates that a disconnection can be detected faster and it is easier to trigger a switchover. A larger value of **hello-interval** indicates that the hot backup relationship is more stable.
- Run the **kplv-pkt** command to configure the format of the heartbeat keepalive packet. If the NAT deployed between ACs, IP packets are not allowed to be routed to the NAT device due to the restriction of the intermediate NAT device. You can run this command to change the format of the heartbeat keepalive packet to the UDP packet to ensure that the heartbeat channel is set up for hot backup.
- Run the **priority level** command to configure the priority of a context. If an AC must be preferentially selected as the active AC, the hot backup priority of this AC must be increased. If an AC is required to support the switchback function, the hot backup priority of this AC must be set to 7.
- If the priority of an AC is high, the AC will be preferentially selected as the active AC when the hot backup connection is set up for the first time. If the AC with the priority set to 7 is selected as the standby AC and completes batch backup of data, a hot backup switchback will be performed and this AC will be changed to the active AC again. A precondition for hot backup switchback is that all APs that are connected with the peer AC also set up connections with the local AC. If the precondition is met and the AC with the priority set to 7 is selected as the standby AC, a hot backup switchback will

be performed within the minimum switchover time (configurable, 10 min by default) after batch backup is completed. Otherwise, a switchback will be performed forcibly 45 minutes after batch backup is completed. Some STAs may go offline due to the forced switchback.

Command	**local-ip** *ip-address*
Parameter Description	*ip-address*: indicates the IP address of the local AC.
Defaults	The IP address of the Loopback 0 interface is used by default.
Command Mode	Hot backup configuration mode
Usage Guide	When the IP address of the local AC changes, the hot backup connection will be interrupted, and then the new IP address of the local AC will be used to set up a hot backup connection.

Command	**work-mode** [**normal** | **quick-switch | cold**]
Parameter Description	**normal**: indicates the normal switchover mode. **quick-switch**: indicates the quick switchover mode.
Defaults	normal
Command Mode	Hot backup configuration mode
Usage Guide	N/A

Command	**hello-interval** *hellointerval*
Parameter Description	*hellointerval*: indicates the heartbeat keepalive period. The unit is ms. The value ranges from 10 to 600,000.
Defaults	The default value is related to the current work mode. When the work mode is normal, the default value is 2s (2000 ms). When the work mode is quick-switch, the default value is 10 ms. After the hierarchical AC function is configured, the default value is 30s (30,000 ms).
Command Mode	Hot backup configuration mode
Usage Guide	The value range is 10 to 600,000. In hierarchical AC scenarios, the value range is 30,000 to 600,000.

Command	**kplv-pkt** [**ip** | **udp**]
Parameter Description	**ip**: indicates that the heartbeat keepalive packet is an IP packet. **udp**: indicates that the heartbeat keepalive packet is a UDP packet.
Defaults	IP packet
Command Mode	Hot backup configuration mode
Usage Guide	N/A

Command	**description** *name*
Parameter Description	*name*: Indicates the name of the hot backup peer.
Defaults	No name is configured.
Command Mode	Hot backup configuration mode
Usage Guide	N/A

Command	**priority level** *priority*
Parameter Description	*priority*: indicates the hot backup priority.
Defaults	The hot backup priority is 4 by default. In hierarchical AC scenarios, the hot backup priority is 7 for a branch AC.
Command Mode	Hot backup context mode
Usage Guide	The priority ranges from 0 to 7. The default priority is 4, and the highest priority is 7. In hierarchical AC scenarios, the hot backup priority is 7 for a branch AC.

Binding the Hot Backup Function with a Context

- (Optional) The configuration is performed on the AC.
- Run the **ap-group** command to bind an AP group with a hot backup context. After the AP group is bound with the hot backup context, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.
- Run the **dhcp-pool** command to bind a DHCP address pool with a hot backup context. If the IP addresses of STAs are on the hot backup AC, you need to bind the DHCP address pool to realize synchronization of DHCP entries between the active and standby ACs. After the DHCP address pool is bound with the context, allocated IP addresses in this DHCP address pool can be synchronized from the active AC to the standby AC.
- Run the **dhcpv6-pool** command to bind a DHCPv6 address pool with a hot backup context. If the IP addresses of STAs are on the hot backup AC, you need to bind the DHCPv6 address pool to realize synchronization of DHCPv6 entries between the active and standby ACs. After the DHCPv6 address pool is bound with the context, allocated IP addresses in this DHCPv6 address pool can be synchronized from the active AC to the standby AC.
- Run the **vrrp interface** command to bind a VRRP group with a context if 802.1x or Web authentication must support the hot backup function. After a VRRP group is bound with a context, the virtual IP addresses in this VRRP group will determine the active/standby relationship based on the hot standby status.

Command	**ap-group** *ap-group*
Parameter Description	*ap-group*: indicates the name of an AP group.
Defaults	No AP group is bound.
Command	Hot backup context mode

Mode	
Usage Guide	N/A

Command	**dhcp-pool** *pool-name*
Parameter Description	*pool-name*: indicates the name of a DHCP address pool.
Defaults	No DHCP address pool is bound.
Command Mode	Hot backup context mode
Usage Guide	You can run the **show wlan hot-backup dhcp-pool config** command to check the binding configurations of a DHCP address pool.

Command	**dhcpv6-pool** *pool-name*
Parameter Description	*pool-name*: indicates the name of a DHCPv6 address pool.
Defaults	No DHCPv6 address pool is bound.
Command Mode	Hot backup context mode
Usage Guide	You can run the **show wlan hot-backup dhcpv6-pool config** command to check the binding configurations of a DHCPv6 address pool.

Command	**vrrp interface** *interface-name* **group** *vrrp-group*
Parameter Description	*interface-name*: indicates the interface corresponding to the VRRP group. *vrrp-group***:** indicates the ID of the VRRP group.
Defaults	No VRRP group is bound.
Command Mode	Hot backup context mode
Usage Guide	You can run the **show wlan hot-backup vrrp config** command to check the binding configurations of a VRRP group.

Enabling Hot Backup

- (Mandatory) The configuration is performed on the AC.
- Unless otherwise specified, the hot backup function must be enabled on both ACs; otherwise, the hot backup function cannot take effect.
- You must ensure the consistency in configurations of the two ACs with the hot backup relationship. In particular, the configuration sequence of interface-mapping configured in AP group configuration mode must be the same on both ACs.

Command	**wlan hot-backup enable**

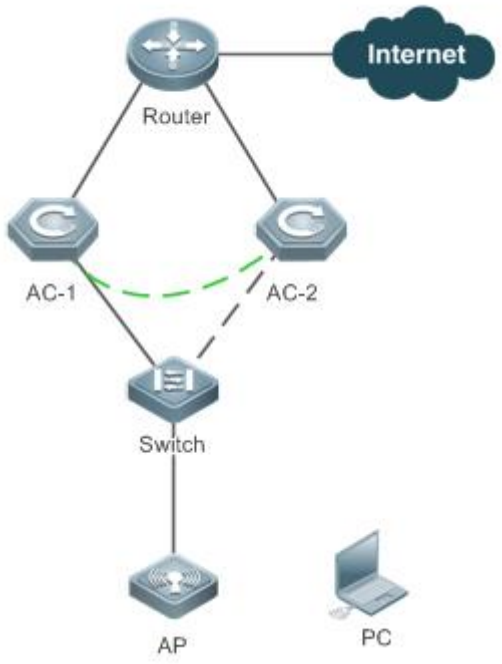
Parameter Description	-
Defaults	The hot backup function is disabled by default.
Command Mode	Hot backup configuration mode
Usage Guide	N/A

Verification

- On the two ACs, check whether the hot backup connection is set up normally, and whether the hot backup status is normal.

Configuration Example

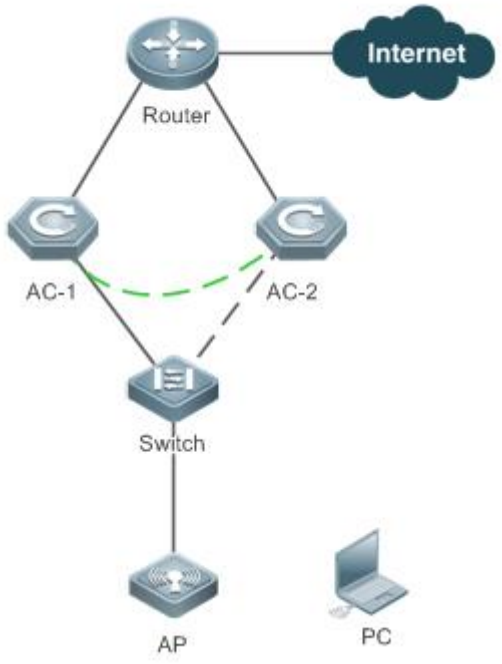
1+1 A/S Networking

Scenario **Figure 1-7**	
Configuration Steps	● Configure the peer IP addresses, including the IP address of AC-1 192.168.1.100 and the IP address of AC-2 192.168.1.200. ● Configure a hot backup context. In the 1+1 A/S networking mode, configure only one context on the two ACs, respectively. Note that the context IDs configured on both ACs must be the same. ● Configure the priority of AC-1 for the hot backup context. ● Configure the associated AP group. Configure the associated AP group "apg-a" in context 10 on both ACs. ● Configure the VRRP group. In the 1+1 A/S networking mode, both ACs have only one context, and the two contexts are in pairs. Therefore, you only need to configure one VRRP group, for example, VRRP

	group 1. Configure VRRP group 1 on the Vlan2 interface of two ACs, respectively. ● Enable the hot backup function.
AC-1	AC-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# priority level 7 AC-1(config-hotbackup-ctx)# ap-group apg-a AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 1 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# ap-group apg-a AC-2(config-hotbackup-ctx)# vrrp interface vlan 2 group 1 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
Verification	After the hot backup relationship is set up between AC-1 and AC-2, check the hot backup configurations.
AC-1	AC-1# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description 192.168.1.200 Enable CHANNEL_UP AC-1# show wlan hot-backup 192.168.1.200 wlan hot-backup 192.168.1.200 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 2000 kplv-pkt : ip ! context 10 hot-backup role : PAIR-ACTIVE

	hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7
AC-2	AC-2# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description 192.168.1.100 Enable CHANNEL_UP AC-2# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 1000 kplv-pkt : ip ! context 10 hot-backup role : PAIR-STANDBY hot-backup rdnd state : REALTIME-SYN hot-backup priority : 4

1+1 A/A Networking

Scenario **Figure 1-8**	
Configuration	● Configure the peer IP addresses, including the IP address of AC-1 192.168.1.100 and the IP address

Steps	of AC-2 192.168.1.200. ● Configure the contexts and bind AP groups with contexts. In the 1+1 A/A networking mode, two contexts must be configured and respectively bound with two AP groups on each of the two ACs. ● Configure the VRRP groups. In the 1+1 A/A networking mode, configure two contexts on each of the two ACs. Assume that VRRP group 1 is configured on Vlan1 interfaces of AC-1 and AC-2, and VRRP group 2 is configured on Vlan2 interfaces of AC-1 and of AC-2. Bind VRRP group 1 with context 10, and VRRP group 2 with context 20. ● Configure the hot backup priorities. For context 10, AC-1 is the active AC and therefore should be configured with the highest priority. For context 20, AC-2 is the active AC and therefore should be configured with the highest priority. ● Enable the hot backup function.
AC-1	AC-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# ap-group apg-a AC-1(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-1(config-hotbackup-ctx)# priority level 7 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# ap-group apg-b AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# ap-group apg-a AC-2(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# context 20 AC-2(config-hotbackup-ctx)# ap-group apg-b AC-2(config-hotbackup-ctx)# vrrp interface vlan 2 group 2

```
AC-2(config-hotbackup-ctx)# priority level 7
AC-2(config-hotbackup-ctx)# exit
AC-2(config-hotbackup)# wlan hot-backup enable
```

Verification After the hot backup relationship is set up between AC-1 and AC-2, check the hot backup configurations.

AC-1

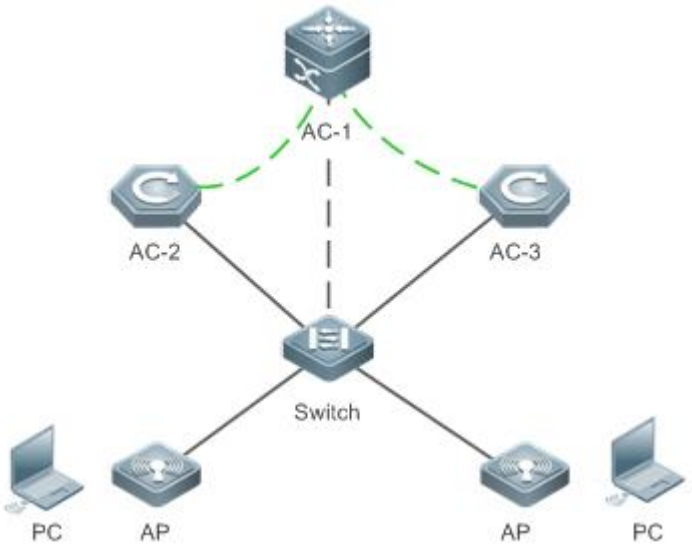
```
AC-1# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- ------------
192.168.1.200        Enable               CHANNEL_UP
AC-1# show wlan hot-backup 192.168.1.200
wlan hot-backup 192.168.1.200
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 7
  !
  context 20
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
```

AC-2

```
AC-2# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-2# show wlan hot-backup 192.168.1.100
wlan hot-backup 192.168.1.100
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-STANDBY
```

```
  hot-backup rdnd state  : REALTIME-SYN
  hot-backup priority    : 4
!
context 20
  hot-backup role        : PAIR-ACTIVE
  hot-backup rdnd state  : REALTIME-SYN
  hot-backup priority    : 7
```

N+1 A/S Networking

Scenario **Figure 1-9**	
Configuration Steps	● Configure the peer IP addresses, including the IP address of AC-1 192.168.1.100, IP address of AC-2 192.168.1.200, and IP address of AC-3 192.168.1.300. Configure two peer IP address on AC-1, and different peer IP addresses correspond to different contexts. ● Configure the contexts and bind AP groups with the contexts. In the N+1 A/S networking mode, one context is configured on each of the *N* ACs, and bound with the corresponding AP group. On the standby AC (AC-1 in this example), *N* contexts must be configured and bound with AP groups on the corresponding active ACs. The AP groups configured on the *N* active ACs cannot conflict with each other. ● Configure the VRRP groups. In the N+1 A/S networking mode, one VRRP group must be configured on each of the *N* active ACs, and *N* VRRP groups must be configured on the standby AC. ● Configure the hot backup priorities. In the N+1 A/S networking mode, the priorities of contexts on the *N* active ACs must be set to the highest priority, and the priorities of contexts on the standby AC can be set to the default value 4.
AC-1	`AC-1# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.`

	AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# ap-group apg-a AC-1(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable AC-1(config-hotbackup)# exit AC-1(config)# wlan hot-backup 192.168.1.300 AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# ap-group apg-b AC-1(config-hotbackup-ctx)# ap-group apg-c AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# ap-group apg-a AC-2(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-2(config-hotbackup-ctx)# priority level 7 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
AC-3	AC-3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-3(config)# wlan hot-backup 192.168.1.100 AC-3(config-hotbackup)# context 20 AC-3(config-hotbackup-ctx)# ap-group apg-b AC-3(config-hotbackup-ctx)# ap-group apg-c AC-3(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-3(config-hotbackup-ctx)# priority level 7

```
AC-3(config-hotbackup-ctx)# exit
AC-3(config-hotbackup)# wlan hot-backup enable
```

Verification

After the hot backup relationship is set up between AC-1 and AC-2 and between AC-1 and AC-3, check the hot backup configurations.

AC-1

```
AC-1# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.200        Enable               CHANNEL_UP
192.168.1.300        Enable               CHANNEL_UP
AC-1# show wlan hot-backup 192.168.1.200
wlan hot-backup 192.168.1.200
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
AC-1# show wlan hot-backup 192.168.1.300
wlan hot-backup 192.168.1.300
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 20
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
```

AC-2

```
AC-2# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-2# show wlan hot-backup 192.168.1.100
wlan hot-backup 192.168.1.100
```

	hot-backup : Enable connect state : CHANNEL_UP hello-interval : 2000 kplv-pkt : ip ! context 10 hot-backup role : PAIR-ACTIVE hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7
AC-3	AC-3# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description 192.168.1.100 Enable CHANNEL_UP AC-3# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 1000 kplv-pkt : ip ! context 20 hot-backup role : PAIR-ACTIVE hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7

Common Errors

- N/A

1.4.2 Configuring Hierarchical AC

Configuration Effect

- Establish hot backup connections in hierarchical AC scenarios.

Notes

- The hierarchical AC roles (center AC and branch ACs) must be configured.
- After the hot backup function is enabled for a branch, the hierarchical AC role and work mode cannot be changed.
- In hierarchical AC scenarios, changing forwarding mode may lead to disconnection and reconnection of the hot backup channel. Hot backup channel cannot be established in central forwarding mode.
- In hierarchical AC scenarios, the quick-switch mode is not supported and the minimum value of **hello-interval** is 30s.

Configuration Steps

Configuring Hierarchical AC Roles

- Hierarchical AC roles must be configured in hierarchical AC scenarios.

Command	**wlan hot-backup [center | branch]**
Parameter Description	**center**: Indicates the center AC. **branch**: Indicates the branch AC.
Defaults	No hierarchical AC role is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the cold Work Mode in Hierarchical AC Scenarios

- Configure the cold work mode on branch ACs that require lightweight backup.
- In cold mode, most data backup with the peer is forbidden and only little data transmission is reserved. When traffic of the center AC is heavy, configure the work mode as cold to reduce the load of the center AC. In cold mode, when a branch AC is faulty, STAs need to be re-associated and STAs' IP addresses need to be obtained again for authentication.

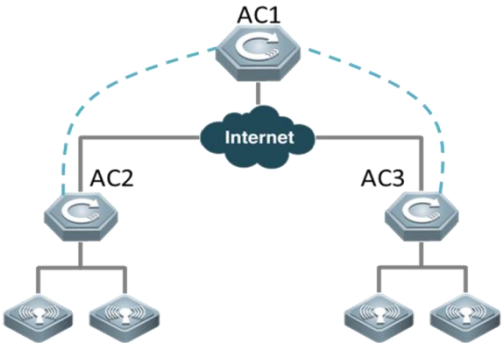
Command	**work-mode cold**
Parameter Description	N/A
Defaults	The work mode is normal by default.
Command Mode	Hot backup configuration mode
Usage Guide	N/A

Verification

- On the center AC and branch ACs, check whether the hot backup connection is normally established and the hot backup status is normal.

Configuration Example

Hierarchical AC Networking

Scenario **Figure 1-2**	
Configuration Steps	● Configure hierarchical AC roles. Configure AC-1 as the center AC and AC-2 and AC-3 as branch ACs. ● Configure peer IP addresses. (The IP address of center AC-1 is 192.168.1.100, the IP address of branch AC-2 is 192.168.1.200, and the IP address of branch AC-3 is 192.168.1.300.) Two peer IP addresses need to be configured on AC-1. Different peer IP addresses correspond to different configuration space. ● Configure description of AC-2 as RD-Office and that of AC-3 as HR-Office. ● Configure the work mode on AC-3 as cold. ● Configure hot backup priorities. In N+1 A/S mode, the highest priority needs to be configured for hot backup instances on branch ACs, and the default priority 4 is configured for the hot backup instances on the center AC.
AC-1	AC-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-1(config)# wlan hot-backup center AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# description RD_Office AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable AC-1(config-hotbackup)# exit AC-1(config)# wlan hot-backup 192.168.1.300 AC-1(config-hotbackup)# description HR_Office AC-1(config-hotbackup)# work-mode cold AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup branch AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# priority level 7 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
AC-3	AC-3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-3(config)# wlan hot-backup branch AC-3(config)# wlan hot-backup 192.168.1.100 AC-3(config-hotbackup)# context 20 AC-3(config-hotbackup-ctx)# priority level 7 AC-3(config-hotbackup-ctx)# exit AC-3(config-hotbackup)# wlan hot-backup enable
Verification	After the hot backup relationship is established between AC-1 and AC-2 or AC-1 and AC-3, display the hot backup configurations.
AC-1	AC-1# show wlan hot-backup layer: center wlan hot-backup peer list: ip address hot-backup state description ------------------ ------------------ ------------------ ----------- 192.168.1.200 Enable CHANNEL_UP RD_Office 192.168.1.300 Enable CHANNEL_UP HR_Office AC-1# show wlan hot-backup 192.168.1.200 wlan hot-backup 192.168.1.200 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 30000 kplv-pkt : ip work-mode : NORMAL !

```
  context 10
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
AC-1# show wlan hot-backup 192.168.1.300
wlan hot-backup 192.168.1.300
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 30000
  kplv-pkt       : ip
  work-mode      : COLD
  !
  context 20
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
```

AC-2

```
AC-2# show wlan hot-backup
layer: branch
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-2# show wlan hot-backup 192.168.1.100
wlan hot-backup 192.168.1.100
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 30000
  kplv-pkt       : ip
  work-mode      : NORMAL
  !
  context 10
    hot-backup role        : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
```

	hot-backup priority : 7
AC-3	AC-3# show wlan hot-backup layer: branch wlan hot-backup peer list: ip address hot-backup state description ---------- ---------- ---------- ---------- 192.168.1.100 Enable CHANNEL_UP AC-3# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 30000 kplv-pkt : ip work-mode : COLD ! context 20 hot-backup role : PAIR-ACTIVE hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7

1.5 Monitoring

Displaying

Description	Command
Displays the global AC hot backup configurations.	**show wlan hot-backup** [*ip-address*]
Displays the context binding configurations of the DCHP address pool and the neighbor address.	**show wlan hot-backup dhcp-pool config** *ip-address*
Displays the context binding configurations of the DCHPv6 address pool and the neighbor address.	**show wlan hot-backup dhcpv6-pool config** *ip-address*

Description	Command
Displays the binding configurations between VRRP groups and contexts under the neighbor addresses.	**show wlan hot-backup vrrp config** *ip-address*

2 Configuring WDS

2.1 Overview

Wireless Distribution System (WDS) is a system enabling interconnection of multiple access points (APs) in wireless bridging or relay mode to interconnect distributed networks and spread wireless signals.

WDS has two working modes: Root Bridge and Non-root Bridge.

- In Root Bridge mode, the wired interfaces connect to wired networks, and the wireless interfaces are used as wireless bridges to connect to those in Non-root Bridge mode.
- In Non-root Bridge mode, the wired interfaces connect to wired networks, and the wireless interfaces are used as wireless bridges to connect to those in Root Bridge mode.

2.2 Applications

Application	Description
Static WDS Bridging	Two separate networks are interconnected via bridging.
Mobile WDS Bridging	A mobile network is interconnected to a static network via WDS bridging.
Automatic Bridging of AP Partners	Wireless signals are spread via bridging between the AP partner and common APs.

2.2.1 Static WDS Bridging

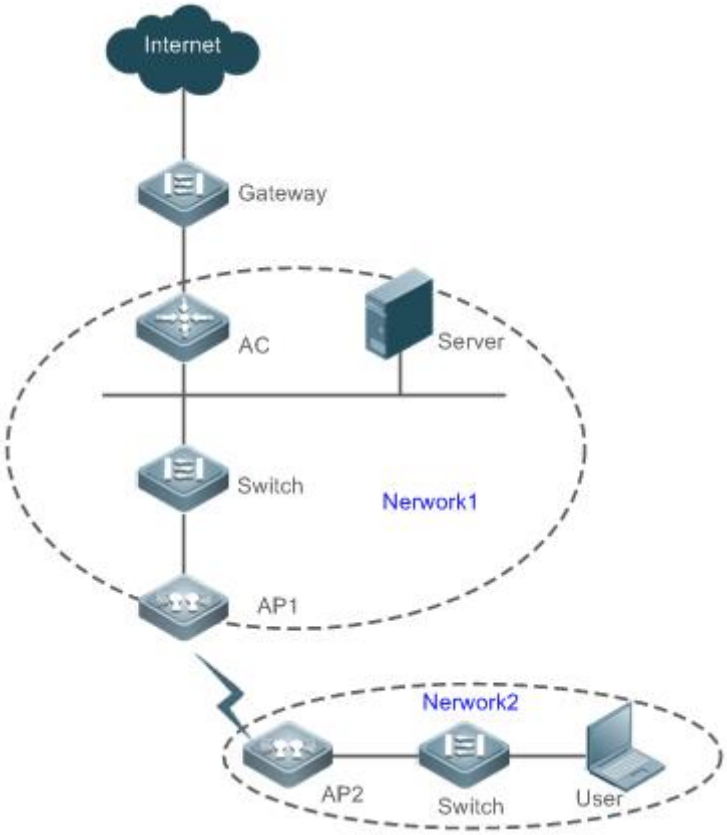
Scenario

Two separate networks are interconnected via bridging.

As shown in the following figure, Network 1 and Network 2 are interconnected via WDS bridging by AP 1 and AP 2.

- WDS bridging enables users in Network 2 to access the server in Network 1.
- WDS bridging also enables users in Network 2 to access the Internet.

Figure 2-1



Remarks	AP 1 is a root bridge. AP 2 is a non-root bridge.

Deployment

- WDS bridging is layer-2 bridging.
- WDS bridging bridges multiple VLANs transparently.

2.2.2 Mobile WDS Bridging

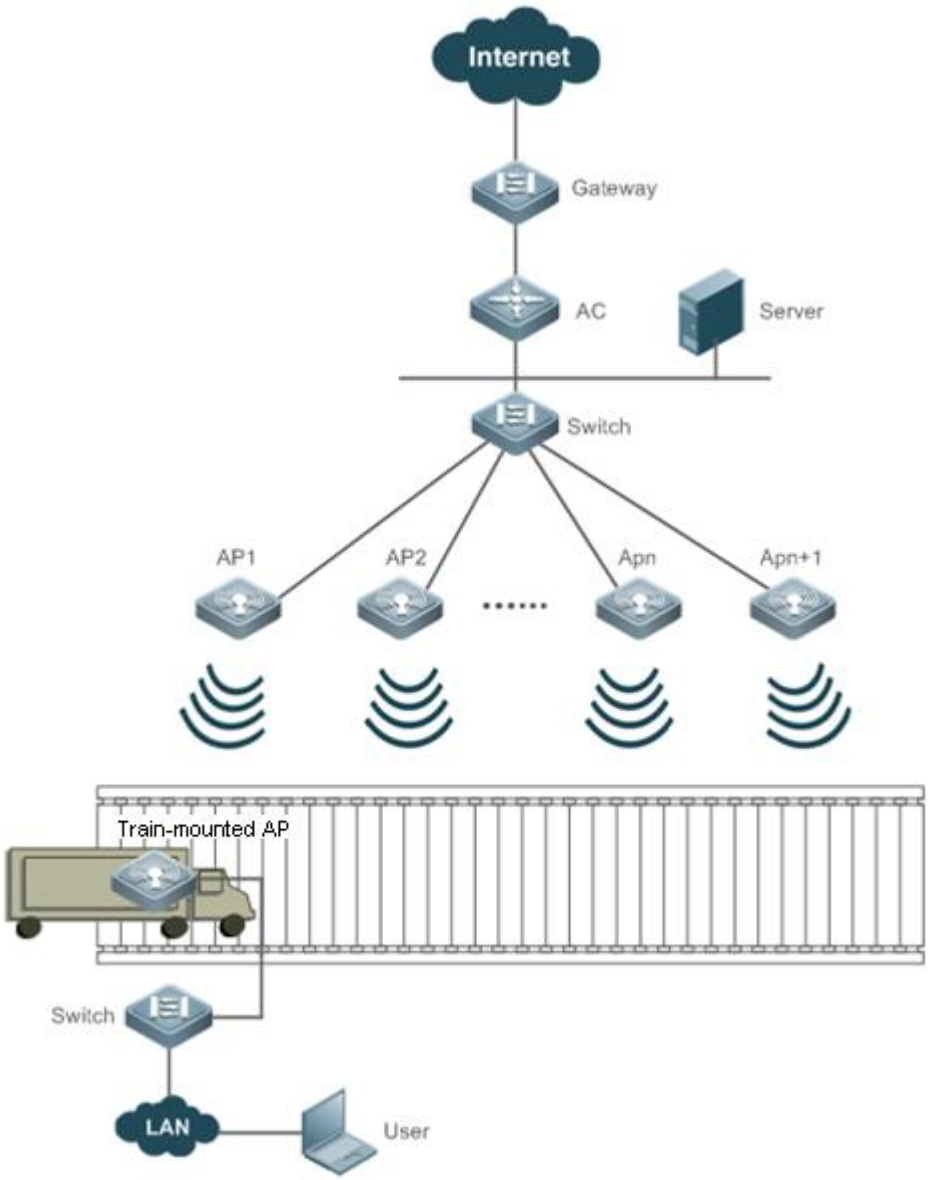
Scenario

A mobile network is interconnected to a static network via WDS bridging.

As shown in the following figure, networks are interconnected via WDS bridging between the train-mounted AP and the APs outside the train (AP 1 to AP n+1).

- When the train is advancing, users in the train can access the Server via bridging.
- When the train is advancing, users in the train can access the Internet via bridging.

Figure 2-2



Remarks	AP 1 to AP n+1 are root bridges. The train-mounted AP is a non-root bridge.

Deployment

- When the train is advancing, the non-root bridge of WDS bridging can roam and switch to a root bridge.
- WDS bridging is layer-2 bridging.
- WDS bridging bridges multiple VLANs transparently.

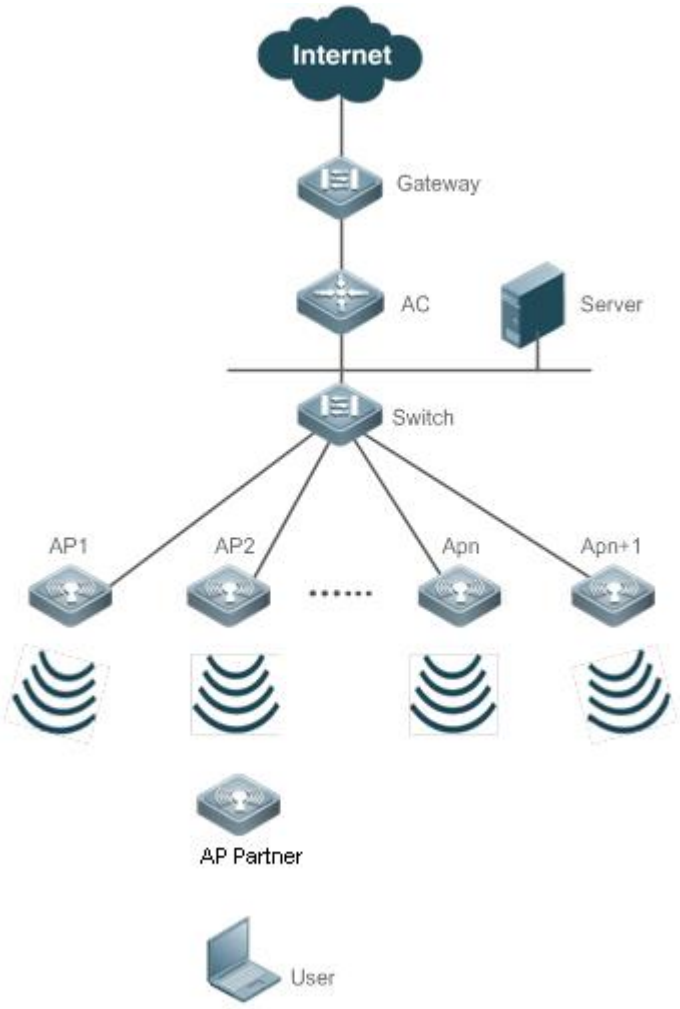
2.2.3 Automatic Bridging of AP Partners

Scenario

An AP partner is used for wireless signal spreading.

As shown in the following figure, wireless signals are spread via bridging between the AP partner and common APs.

Figure 2-3



Deployment

- The AP partner is used to achieve a large coverage of wireless signals.
- The AP partner enjoys zero-configuration.
- When automatic bridging is configured, the AP partner automatically accesses the network.

2.3 Features

Basic Concepts

Root Bridge

A root bridge is the root node in WDS bridging. It allows the access of a non-root bridge to establish WDS bridging.

Non-root Bridge

A non-root bridge is a non-root node in WDS bridging. It actively accesses the root bridge to establish WDS bridging based on user configuration.

Features

Feature	Description
Establishing WDS Bridging	Establishes WDS bridging.
Address Format of MAC Frames in WDS	Describes the address format of MAC frames exchanged between the root and non-root bridges in WDS.

2.3.1 Establishing WDS Bridging

Establish WDS bridging.

Working Principle

Each AP is a Basic Service Set (BSS). Each has a BSSID (which is usually the MAC address of an AP). An AP regularly broadcasts Beacon frames with the SSID (name of the WLAN) and BSSID, and wireless stations (STAs) listen to the Beacon frames by scanning. If the SSID of a Beacon frame is the same as the network name preset by an STA, the STA accesses the network of the AP. If multiple APs are eligible with their Beacon frames listened, the STA selects one of the APs for access. The access process is that the STA connects and associates the selected AP by recognizing the BSSID of the AP.

In WDS, the root bridge will specify a BSS used for the access of non-root bridges to establish bridging. Common STAs are not allowed to access this BSS. Only when such BSS exists will the root bridge accept the access request of a non-root bridge. During access, the root bridge will provide a mechanism to determine whether to admit a non-root bridge into its network.

For a non-root bridge, accessible root bridges are searched based on the configured BSSIDs or SSIDs. A mechanism will be provided in the searching process to determine whether a root bridge with a specified BSSID or SSID is accessible. The root bridge will be connected if accessible. In this way, WDS bridging is established.

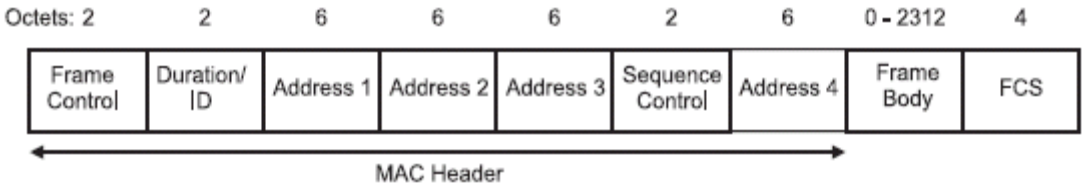
2.3.2 Address Format of MAC Frames in WDS

This section describes the address format of MAC frames exchanged between a root bridge and a non-root bridge in WDS bridging.

Working Principle

In IEEE 802.11 standards, the format of MAC frames is defined for the wireless technology which consists of a MAC header with four address fields, as shown below:

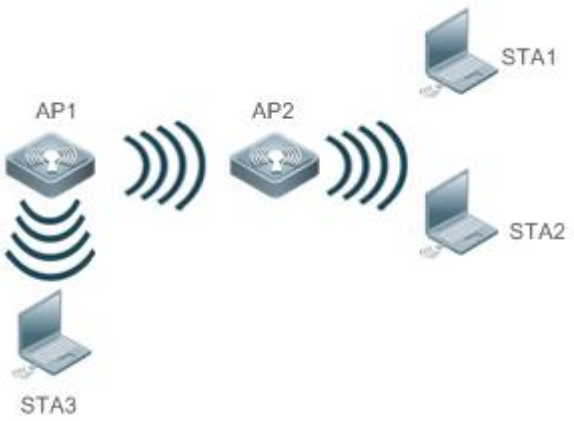
Figure 2-4



Based on the transmission modes, 802.11 MAC frames can be in three-address format or four-address format. The MAC frames in three-address format are transmitted between APs and STAs; while the MAC frames in four-address format are transmitted between APs.

As shown in the following figure, when STA 1 communicates with STA 2, STA 1 sends a MAC frame with three address fields of AP 2, STA 1 and STA 2 to AP 2 (See STA 1->AP 2 in the table). After receiving the MAC frame, AP 2 forwards it to STA 2, with three address fields changed into the MAC addresses of STA 2, AP 2 and STA 1 (see AP 2->STA 2 in the table). When STA 1 communicates with STA 3, after receiving a MAC frame from STA 1, AP 2 needs to forward it to AP 1, so the three-address format is changed to a four-address format, with the MAC addresses of AP 2, AP 1, STA 3 and STA 1 filled (see Figure 2-5). After receiving the frame, AP 1 forwards it to STA 3 and changes the four-address format back to a three-address format.

Figure 2-5



Transmission Mode	Address 1	Address 2	Address 3	Address 4
STA 1 -> AP 2	RA = AP 2	TA = STA 1	DA = STA 2	N/A
AP 2 -> STA 2	RA = STA 2	TA = AP 2	SA = STA 1	N/A
AP 2 -> AP 1	RA = AP 1	TA = AP 2	DA = STA 3	SA = STA 1

2.4 Configuration

Configuration	Description and Command
Configuring WDS Basic	(Mandatory) It is used to establish WDS bridging.

Functions	**station-role root-bridge bridge-wlan**	Configures a root bridge.
	station-role non-root-bridge	Configures a non-root bridge.
	parent	Specifies a root bridge for a non-root bridge.
	⚠ Mandatory if a non-root bridge works in fit AP mode. It is used for WDS pre-configuration.	
	wds pre-config	Pre-configures a fit non-root bridge.
	⚠ Mandatory if non-root configuration is to be modified on the AC. It is used to submit or delete the inactive WDS's commands.	
	wds config	Submits or clears inactive configuration of non-root bridges.
	⚠ (Optional) It is used to configure WDS parameters or enable the bridge coverage.	
	bridge roam-threshold	Configures the roaming thresholds of a non-root bridge.
	bridge with-client	Configures bridge coverage.
	bridge vlan	Creates a bridge VLAN.
	bridge security	Configures bridge encryption on a non-root bridge.
	wds security enable	Enables bridge encryption.
	wds-mode enable	Enables WDS bridge mode.
	autowds	Enables automatic bridging of AP partners.

2.4.1 Configuring WDS Basic Functions

Configuration Effect

- Configure WDS bridging.

Notes

- In WDS application environments, the Multiple Spanning Tree Protocol (MSTP) function must be enabled to prevent potential network loops.
- Meanwhile, the Address Resolution Protocol (ARP) agent must be disabled.
- The WDS configuration commands can be used for bridging establishment only. They must collaborate with other commands to build a test environment, such as the commands for BBS creation or wireless interface configuration.
- In WDS, the fit APs need to support Control and Provisioning of Wireless Access Points (CAPWAP) by Bridge-Group Virtual Interface (BVI) by default.

Configuration Steps

↘ **Configuring the WDS Mode**

- Mandatory.
- Configure the WDS bridge mode on ACs for fit APs.
- Run the **wds-mode enable** command to configure an AP to work in WDS bridge mode.

Command	**wds-mode {enable | disable}**
Parameter Description	**enable**: Enables the WDS bridge mode. **disable**: Disables the WDS bridge mode.
Defaults	The WDS bridge mode is disabled by default.
Command Mode	AP configuration mode on the AC
Usage Guide	Run the **show ap-config wds-mode summary** command on the AC to check whether the WDS mode is enabled for the corresponding AP. Run the **show wds-mode** command on the AP to check whether the WDS mode is enabled for the corresponding AP. AP will restart after the command is executed.

Configuring a Root Bridge

- Mandatory.
- Configure bridge coverage on ACs for fit APs.
- Run the **station-role root-bridge bridge-wlan** *wlan-id* command to configure an AP working in the mode of WDS bridging.
- Specify a WLAN to bridge BSSs. If the WLAN has not been created, WDS bridging cannot work.

Command	**station-role root-bridge bridge-wlan** *wlan-id* [**radio** *radio-id*]
Parameter Description	**bridge-wlan** *wlan-id*: Specifies a bridge WLAN. **radio** *radio-id*: Specifies a radio.
Defaults	root-ap configuration mode
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring a Non-Root Bridge

- Mandatory.
- Configure bridge coverage on ACs for fit APs.
- On a non-root bridge, you must specify a radio to work in the Non-root Bridge mode.
- Run the **station-role non-root-bridge** command to configure an AP working in the Non-root Bridge mode of WDS bridging.
- A non-root bridge starts to establish and process WDS bridging only after a destination root bridge is specified.

Command	**station-role non-root-bridge** [**radio** *radio-id*]
Parameter Description	**radio** *radio-id*: Specifies a radio.

Defaults	root-ap configuration mode
Command Mode	AP configuration mode
Usage Guide	The configurable VLAN number varies with the product model.

Specifying a Root Bridge for a Non-root Bridge

- Mandatory.
- Configure bridge coverage on ACs for fit APs.
- Two ways are available for specifying a root bridge to access: specifying its BSSID or SSID.
- Specifying the BSSID of a root bridge: This is applicable to a static root bridge.
- Specifying the SSID of a root bridge: This will enable the non-root roaming function to select the root bridge with the best signals for access.
- Run the **parent** { **mac-address** *HHHH.HHHH.HHHH* | **ssid** *ssid* } [**channel** *channel* **chan-width** *chan-width*] command to specify the BSSID or SSID of a root bridge to be accessed by a non-root bridge.

Command	**parent** { **mac-address** *HHHH.HHHH.HHHH*	**ssid** *ssid* } [**radio** *radio-id*]
Parameter Description	**mac-address** *HHHH.HHHH.HHHH*: Specifies the BSSID of a root bridge for static bridging. **ssid** *ssid*: Specifies the SSID of a root bridge optimal for roaming. **radio** *radio-id*: Specifies a radio.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Non-root bridges start searching root bridges after this command is executed. If WDS bridging is required, this command must be configured on the non-root bridges.

Configuring the Roaming Thresholds of a Non-Root Bridge

- Optional.
- Configure bridge coverage on ACs for fit APs and on APs for fat APs.
- This command is configured to adjust roaming parameters.
- Generally, the configuration of these thresholds is not required unless in special environments (where the roaming parameters need to be adjusted).
- This command requires professionals to propose suitable configuration after measuring and analyzing the application environments. It is not recommended to configure this command without the assistance of professionals; otherwise, the WDS's roaming effect and even the use of WDS bridging will be affected.

Command	**bridge roam-threshold** *num1 num2 num3 num4* [**radio** *radio-id*]
Parameter Description	*num1*: Roaming start threshold, 40 by default. *num2*: Scanning start threshold, 15 by default. *num3*: Roaming switch threshold, 5 by default.

	num4: Roaming switch time threshold, 5 by default. **radio** *radio-id*: Specifies a radio.
Defaults	Enabled.
Command Mode	AP configuration mode
Usage Guide	Generally, the configuration of these thresholds is not required unless in special environments (where the roaming parameters need to be adjusted).

Configuring Bridge Encryption on a Non-Root Bridge

- Optional.
- Configure bridge coverage on ACs for fit APs.
- This command is configured to adjust encryption parameters.
- This configuration is required only when bridging is required for accessing an encrypted network.
- The encryption parameters must be configured the same as those of the encrypted network to be accessed; otherwise, the bridging may fail.

Command	**bridge security** [**radio** *num*] { **wpa** | **rsn** } **ciphers** { **aes** } **akm psk key** { **ascii** | **hex** } *key*
Parameter Description	**radio** *num*: Indicates a configured RF port. **wpa | rsn**: Configures WPA or RSN authentication. **aes**: Configures AES encryption. **psk**: Configures PSK access authentication. **ascii**: Specifies ASCII as PSK format. **hex**: Specifies Hex as PSK format. *key*: When the ASCII form is selected, the key has a length ranging from 8 to 63 ASCII characters. When the Hex form is selected, the key has a length with 64 hexadecimal characters.
Defaults	No encryption parameter is configured.
Command Mode	Fat AP: AP configuration mode
Usage Guide	The encryption parameters must be configured the same as those of the encrypted network to be accessed; otherwise, the bridging may fail.

Creating or Creating a Bridge VLAN

- Optional.
- This is configured only on ACs in fit AP mode.
- If you need to create a VLAN independently on an AP, you must conduct this configuration on the AC.

Command	**bridge vlan** *vid*
Parameter Description	*vid*: ID of the VLAN to be created
Defaults	N/A

Command Mode	AP configuration mode
Usage Guide	Use this command to create a WDS VLAN in coordination with other VLAN creation commands.

Configuring Bridge Coverage

- Optional.
- In Root Bridge mode: Configure bridge coverage on ACs for fit APs. In Non-root Bridge mode: Configure bridge coverage on APs for fit APs by pre-configuration.
- This command is optional if the WDS does not need the bridge coverage function. This command is mandatory if the bridge coverage function is required.
- This command is not recommended so that the coverage function is disabled during bridging.

Command	**bridge with-client{ enable** | **disable** } [**radio** *radio-id*]
Parameter Description	**enable**: Enables bridge coverage. **disable**: Disables bridge coverage. **radio** *radio-id*: Specifies a radio.
Defaults	Bridge coverage is disabled by default.
Command Mode	AP configuration mode
Usage Guide	It is recommended to disable bridge coverage.

Configuring the Front and Back Channels of a Non-root Bridge

- Optional.
- This function is configured on non-root bridge scenarios like subway trains where the front and back of AP channels may be changed.
- After this commanded is configured, the channel of a non-root bridge changes based on the working status.

Command	**wds head-chan** *num1* **tail-chan** *num2* [**radio** *radio-id*]
Parameter Description	*num1*: Front channel *num2*: Back channel **radio** *radio-id*: Specifies a radio.
Defaults	Disabled.
Command Mode	Fit AP: Interface configuration mode Fat AP: AP configuration mode
Usage Guide	This is configured only on the non-root bridges. Configure this function on a non-root fat AP directly in fat AP mode and on the in fit AP mode. Only after being committed will the configuration take effect.

Enabling Bridge Encryption

- Optional.

- This is configured when the non-root and root bridges need encrypted communication in WDS.
- This command must be consistently configured on the root and non-root bridges, otherwise, the communication fails.

Command	**wds security enable**[**radio** *radio-id*]
Parameter Description	**radio** *radio-id*: Specifies a radio.
Defaults	Bridge encryption is disabled by default.
Command Mode	Fat AP: AP configuration mode
Usage Guide	On the AC, configuration is directly pushed for root bridges and pushed only after being committed for non-root bridges.

Pre-configuring a Fit Non-root Bridge

- Optional.
- When a non-root bridge needs to work in fit AP mode, the pre-configuration must be conducted on fat APs.
- First of all, conduct required non-root configuration (including configuring the working mode as NONROOT-BRIDGE and specifying information on the root bridges to be accessed).

Command	**wds pre-config**[**delete**] [**radio** *radio-id*]
Parameter Description	**delete**: Deletes pre-configuration. **radio** *radio-id*: Specifies a radio.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	In turn, to exit the bridging mode, run the **wds pre-config delete** command to delete the non-root pre-configuration.

Clearing or Submitting Inactive WDS Configuration

- Optional.
- Use this command to submit inactive commands.
- Changes in the configuration of non-root bridges on the AC cannot take effect immediately. To issue the changes, you must run the **wds config commit** command.

Command	**wds config**[**clear | commit**] **radio** *radio-id*
Parameter Description	**clear**: Clears inactive WDS configuration. **commit**: Submits inactive WDS configuration. After submitting, the bridging will be re-established. **radio** *radio-id*: Specifies a radio.
Defaults	N/A
Command Mode	AP configuration mode

Enabling Automatic Bridging of AP Partners

- Optional.
- This command can be configured in all/standalone AP configuration mode (single AP), or AP group configuration mode, with the priority order: standalone AP configuration mode > AP group configuration mode > all AP configuration mode.
- After this command is configured and a root AP receives a request from the AP partner (non-root), WDS is created automatically.

Command	**autowds**
Parameter Description	N/A
Defaults	Automatic bridging is disabled by default.
Command Mode	All/standalone AP configuration mode or AP group configuration mode
Usage Guide	This function is required not for normal non-root bridges but for AP partners.

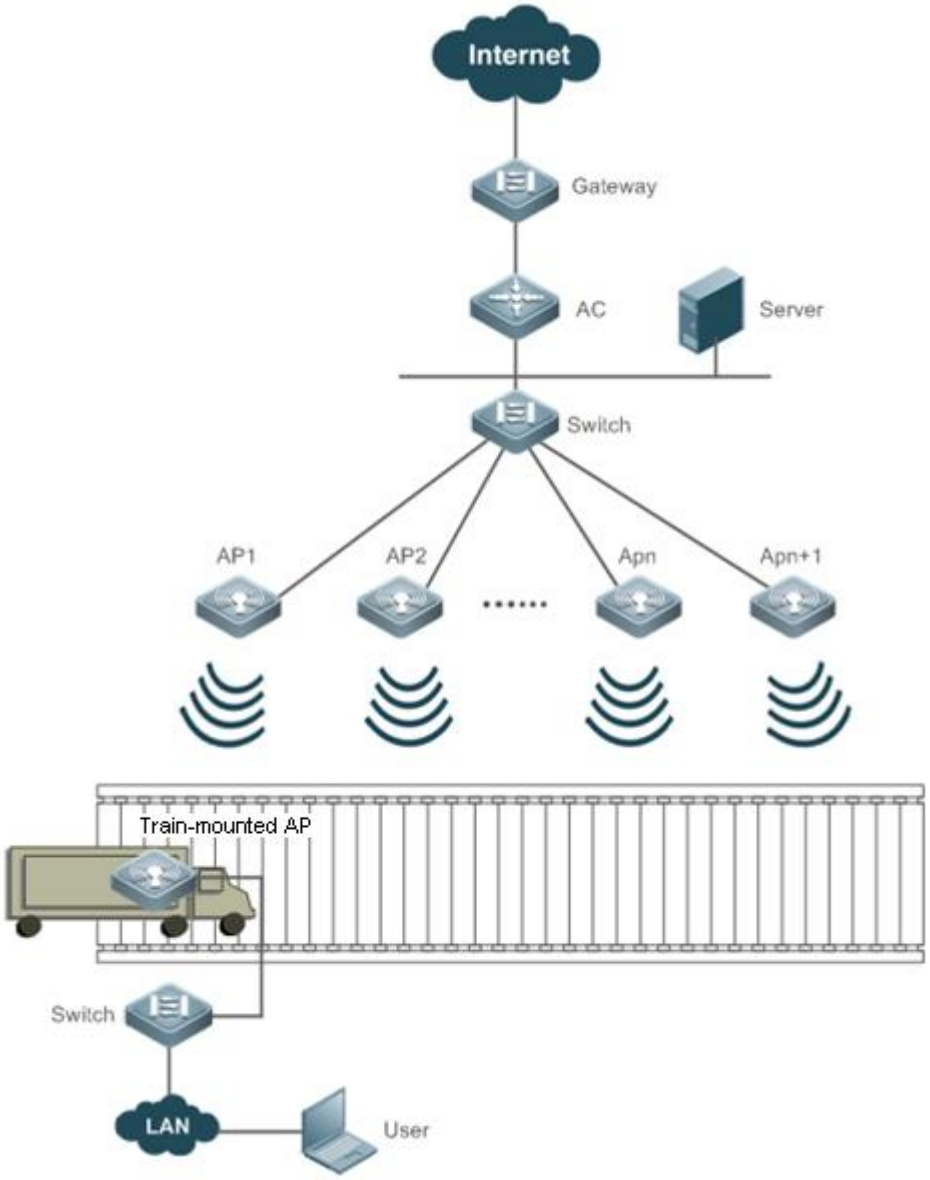
Verification

run the **show** command to display WDS configuration.

Configuration Example

WDS Roaming Scenario in Fit AP Mode

In this scenario, APs are required to establish a CAPWAP link through BVI by default.

Scenario **Figure 2-6**	
Configuration Steps	● Configure the WLAN, VLAN, and channels for AP 1 to AP n+1. (This scenario needs a unified channel.) ● The above configuration is the same as that in common AP application scenarios. ● Configure the WDS's root bridges and specify a WLAN used for bridging. ● Configure the WDS's non-root bridge. Pre-configuration is used for the non-root bridge. (Assuming that the bridge WLAN is **ruijie-root** and the channel is 149 with the bandwidth of 40 MB)
ROOT **(AP1 - APn+1)**	Ruijie#configure terminal Ruijie(config)#ap-config ap1 Ruijie(config-ap)# station-role root-bridge bridge-wlan 1 radio 2

NONROOT (In-vehicle AP)	Ruijie#configure terminal Ruijie(config)#interface dot 2/0 Ruijie(config-if-Dot11radio 2/0)# station-role non-root-bridge Ruijie(config-if-Dot11radio 2/0)# parent ssid ruijie-root Ruijie(config-if-Dot11radio 1/0)# wds pre-config create Ruijie(config-if-Dot11radio 1/0)# exit Ruijie(config)#ap-mode fit
Verification	Run the following command to display WDS bridging information.
In-vehicle AP	Ruijie#show dot11 wds-bridge-info 1/0 WDS-MODE: NONROOT-BRIDGE MAC:00d0.f822.3304 WBI 1/0 ROOT 32d0.f822.3303
On the AC	Display WDS bridging information on the interface. Ruijie#show ap-config wds-bridge-info summary Ap Name Mac Address Radio Station Role ---------- ---------- ----- ---------- Ap-001 00d0.f822.3301 2 ROOT-BRIDGE Ap-002 00d0.f822.3304 2 NON-ROOT-BRIDGE Ruijie# show ap-config wds-bridge-info Ap-001 radio 2 WDS-MODE: ROOT-BRIDGE BRIDGE-WLAN: Status OK WlanID 1, SSID ruijie_root, BSSID 32d0.f822.3303 WBI 1/0 NONROOT 00d0.f822.3304

Common Errors

N/A

2.5 Monitoring

Displaying

Description	Command
Displays the WDS bridge configuration on an AP.	**show wds-mode**
Displays the WDS bridge configuration on an AC.	**show ap-config wds-mode summary**
Displays WDS links on an AC.	**show ap-config wds-bridge-info** { **summary** |*ap-name* **radio** *radio-id* }
Displays WDS configuration on an AC.	**show ap-config wds-config** [*ap-name*]

3 Configuring RIPT

3.1 Overview

The Remote Intelligent Perceptive Technology (RIPT) is also known as the smart AP technology. As a wireless network edge device (as compared with an AC), the smart AP can perceive its connection with the AC and take over external provision of wireless networks seamlessly once connection fails. The wireless RIPT solution can be deployed in enterprise branch networks for the availability and sustainability of inter-WAN networks between the AC and APs in case of faults. It can also be deployed in a Wireless Local Area Network (WLAN) network to reduce reliance on ACs and improve its availability.

Protocols and Standards

N/A

3.2 Applications

Application	Description
Deploying RIPT in a WLAN network	Both the AC and APs are deployed in a Local Area Network (LAN) network.
Deploying RIPT in enterprise branch networks	The AC is deployed in the enterprise headquarters, while APs are deployed in various branches and connected to the AC through a WAN network.

3.2.1 Deploying RIPT in a WLAN Network

Scenario

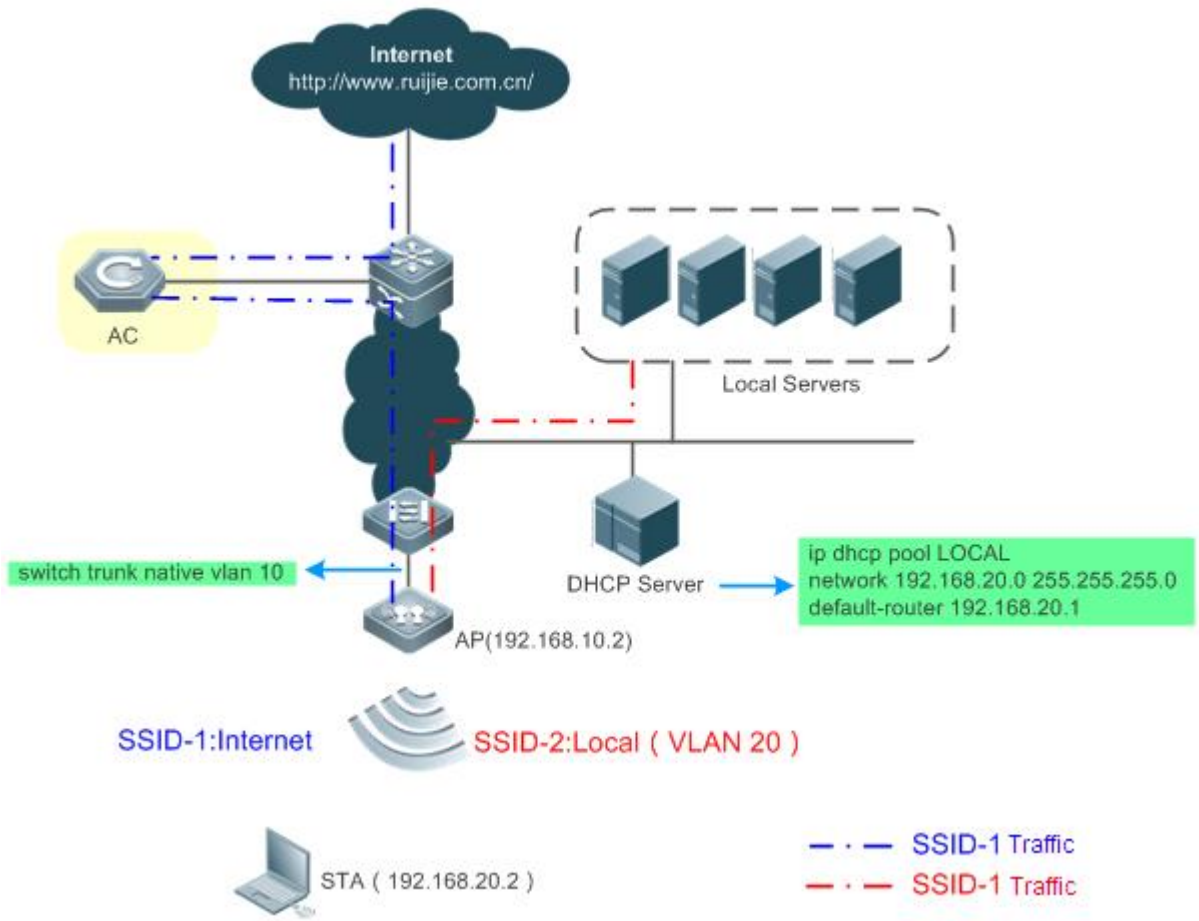
The following are two types of RIPT WLANs to meet service requirements:

- WLAN for operators' Internet services: applies centralized forwarding and 802.1x/Web authentication mode. There is potential demand for accounting.
- WLAN for LAN resource services: applies local forwarding and WAP\WAP2-PSK authentication mode.

When the AC is unreachable (such as restart or outage), the wireless network can still access local resources.

For example, as shown in Figure 3-1, the AC is unreachable while the other devices such as switches and APs are normal. The WLAN service is not affected and continues to be available.

Figure 3-1



Remarks	The DHCP server for allocating an IP address to the STA cannot be configured on the AC. The AC cannot forward data traffic for SSID-2 that uses local forwarding.

Corresponding Protocols

- Create a WLAN, and configure the forwarding mode and the security policy.
- Enable RIPT on the APs.

3.2.2 Deploying RIPT in Enterprise Branch Networks

Scenario

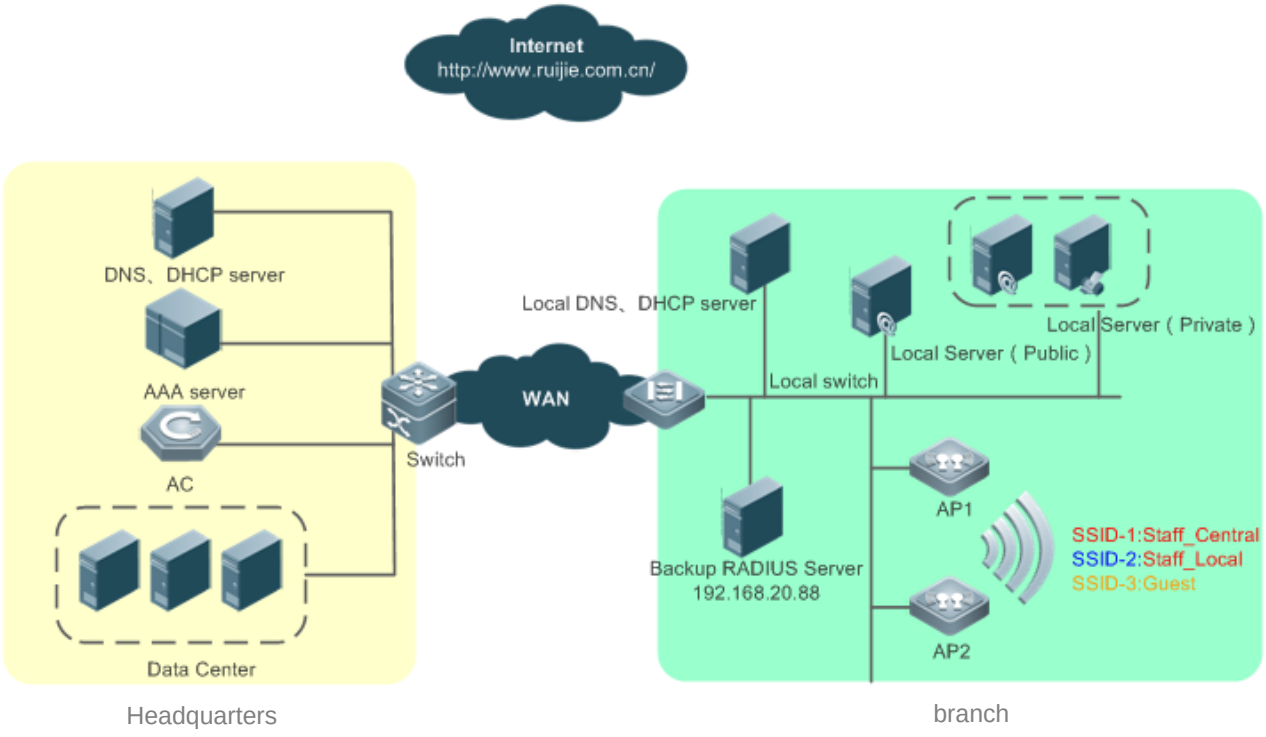
The following are requirements for the enterprise branch networks:

- An AC is deployed in the headquarters data center, while some APs and a DHCP server are deployed in the branches to serve STAs.
- A RADIUS server is deployed in the headquarters to perform access authentication for STAs in both the headquarters and all branches. If a backup RADIUS server is not deployed in the branch, access authentication for STAs in the branch fails when the APs in the branch are disconnected from the headquarters AC (for example, when the WAN fails).

- Traffic for accessing the headquarters data center will pass the WAN between the branch and the headquarters, whereas traffic for accessing local resources and Internet resources of the branch is forwarded in the branch instead of passing the WAN.

As shown in Figure 3-2, when the route from a branch AP to the headquarters AC is unreachable, the branch AP can still provide network for local resource access or the like.

Figure 3-2



Remarks	The AC is deployed in the headquarters and connected with APs through the WAN. A DHCP server for IP address allocation is deployed in the branch. If there is no backup RADIUS server in the branch, STA access authentication will stop when the WAN link fails. If 802.1X authentication is adopted, another WLAN can be deployed and the function of SSID enabling after connection interruption can be enabled, so that the WLAN can provide network services for new STAs when the AP connection is interrupted. Free Web authentication after connection interruption can be enabled to ensure that Web-authenticated STAs can access the network after the AP connection is interrupted.

Deployment

- Deploy a WLAN for employees in the branch to access the headquarters data center. Enable the centralized forwarding mode. The STA access authentication runs in the headquarters.
- Deploy a WLAN for employees in the branch to access Internet resources and local resources. Enable the local forwarding mode and the 802.1x local authentication. When an AP works in connected mode, the headquarters RADIUS server performs the authentication. When the AP works in standalone mode, another WLAN can be deployed

and the function of SSID enabling after connection interruption can be enabled, so that the WLAN can provide network services for new STAs; or the 802.1X authentication is prohibited for the new STAs for the security purpose.

- Deploy a WLAN for guest access on Internet resources and public resources of the branch. Enable the local forwarding mode and the Web local authentication. When an AP works in connected mode, the headquarters RADIUS server performs the authentication. When the AP works in standalone mode, free Web authentication can be enabled to ensure that new STAs can access the network.
- Create an AP group, and configure WLAN to VLAN mapping.
- Configure the APs, add them to the AP group, and enable the RIPT function.

3.3 Features

Basic Concepts

Connected Mode and Standalone Mode

When a CAPWAP tunnel has been established between an AP and an AC, the working environment of the AP is referred to as connected mode.

When the CAPWAP tunnel between the AP and the AC is broken, the working environment of the AP is referred to as standalone mode.

RIPT AP

An RIPT-enabled AP is called an RIPT AP. It is also known as a smart AP.

AC Configuration Change Monitoring

After re-establishing a CAPWAP tunnel in standalone mode with the AC, an RIPT AP should check the AC configuration change, so as to determine whether to maintain the online status of online STAs accordingly. Therefore, AC configuration should be monitored, so as to determine whether it has changed when the RIPT AP is offline.

A configuration change is considered as having taken place when one of the following operations is performed:

- The AC enters the configuration mode with CLI commands, or a CLI command has been executed in the configuration mode.
- A SET operation has been performed on the AC through SNMP.

If either of the above two cases occurs on the AC when the AP is offline, the configuration of the AC is considered as having changes. Then online STAs will be brought offline when the AP is reconnected to the AC.

In case all configuration of the AC has been stored in its Flash memory, when the AC is restarted (or powered on following powered off) and the configuration file in the Flash memory does not change, the configuration of the AC is considered as having no change.

Overview

Feature	Description

Enabling the RIPT Function	The AP automatically detects its connection to the AC. When the connection to the AC is broken, the AP continues to provide services by smoothly switching to the standalone mode.
Enabling SSID After Connection Interruption	After the AP connection is interrupted, the WLAN provides SSID signals for STAs to access the network. In normal cases, this function is used together with 802.1X authentication.
Enabling Free Web Authentication After Connection Interruption	After the AP connection is interrupted, STAs can access WLANs adopting Web or MAB authentication without performing Web or MAB authentication.

3.3.1 Enabling the RIPT Function

An AP becomes an RIPT AP only after the RIPT function is enabled. When the AP detects that its connection to the AC is broken, the AP automatically switches to the standalone mode. After a connection to the AC is re-established, the AP switches back to the connected mode.

Working Principle

When the WLAN is set to the local forwarding mode, an RIPT AP has the same the working mechanism with a common fit AP in connected mode. The AC performs STA association and authentication. After a new STA gets online, the AC backs up its information in real time to the associated RIPT AP. Then the RIPT AP creates STA information and a backup entry. When detecting that its CAPWAP connection to the AC is broken, the RIPT AP automatically switches to the standalone mode. After that, online STAs will maintain their online status while new STAs can get online. If the WLAN works in centralized forwarding mode, online STAs will be brought offline and SSID broadcast is automatically disabled.

In standalone mode, the RIPT AP will first detect whether the AC configuration changes after re-establishing a CAPWAP tunnel with the AC. If the configuration of the AC does not change, the RIPT AP synchronies information about all online STAs to the AC, so that the AC re-establishes STA information. After that, STA association and authentication is switched back to the AC while the RIPT AP enters the connected mode. If the configuration of the AC has changed, the RIPT AP brings offline all online STAs, receives the new configuration, and then enters the connected mode.

3.3.2 Enabling SSID After Connection Interruption

When the AP connects to the AC, STAs cannot discover SSID or access the network. When the connection between the AP and AC is interrupted, SSID is enabled for STAs to access the network. After the connection between the AP and AC recovers, the SSID becomes unavailable.

This function is used as a supplementary solution for RIPT APs adopting 802.1X authentication. After the RIPT AP connection is interrupted, network access requests from STAs using 802.1X authentication cannot be processed. To enable STAs to access the network, configure another WLAN and enable this function.

Working Principle

If the function of SSID enabling after connection interruption is enabled STAs can access the network after the AP is disconnected. After the AP connection is recovered, if the function of SSID enabling after connection interruption is enabled for the WLAN, the WLAN stops working, STAs are not allowed to access the network and online STAs become offline.

3.3.3 Enabling Free Web Authentication After Connection Interruption

When the AP connects to the AC, STAs can access the network only after Web or MAB authentication. When the connection between the AP and AC is interrupted, STAs can access the network without Web or MAB authentication. After the connection between the AP and AC is recovered, STAs can access the network after Web or MAB authentication.

Working Principle

An RIPT AP determines whether free Web authentication is enabled for the WLAN after the AP connection is interrupted. If this function is enabled for the WLAN, STAs can directly access the network. After the AP connection is recovered, STAs can access the network only after authentication.

3.4 Configuration

Configuration	Description and Command	
Configuring the RIPT Function	⚠ Mandatory configuration. Enable the RIPT function.	
	ript enable	Enables the RIPT function.
	⚠ Optional configuration. Enable SSID after connection interruption.	
	enable-ssid at-capwap-down	Enables SSID after connection interruption.
	⚠ Optional configuration. Enable free Web authentication after connection interruption.	
	free-webauth at-capwap-down	Enables free Web authentication after connection interruption.

3.4.1 Configuring the RIPT Function

Networking Requirements

- An RIPT AP can independently work when its connection to the AC is broken.
- The moment that the RIPT function is enabled or disabled, the AP actively breaks its CAPWAP connection to the AC and then re-establishes a new connection. This also happens when the AP gets online for the first time.
- After SSID is enabled after connection interruption, the WLAN works only after the AP connection is interrupted.
- After free Web authentication is enabled for a WLAN, STAs can access the network without Web or MAB authentication after the AP connection is interrupted.

Notes

- Save the configuration before restarting the AC. If the configuration is not yet saved before the AC is restarted, the restarted AC will use the configuration stored in its Flash memory. In this case, the configuration used on the RIPT AP is different from that being used on the AC after the restart and the situation is handled the same as when the AC configuration has changed. Therefore, make sure to save the configuration before restarting the AC in the RIPT scenario.

- In 802.1X authentication scenarios, STAs are not allowed to access WLANs adopting 802.1X authentication after the AP connection is interrupted.
- Configure the keep-alive time of APs. For an RIPT-enabled AP, you need to configure its keep-alive time according to the status of the previous network communications between the AP and the AC. For details, see the configuration command **echo-interval** to be executed in AP configuration mode. The purpose of doing so is to avoid instability of the CAPWAP tunnel between the AP and the AC, which may occur as a result of poor network communications between the AP and the AC.
- Certain requirements must be met during the deployment of the DHCP server. If an RIPT AP or STA acquires its IP address through DHCP and the RIPT AP works in standalone mode, the DHCP server must be reachable for the RIPT AP and STA.

Configuration Steps

Creating a WLAN and Setting It to the Local Forwarding Mode

- Mandatory configuration. If the WLAN works in centralized forwarding mode, STAs will be brought offline after the RIPT AP switches to the standalone mode.
- Create the WLAN in global configuration mode on the AC.
- By default, the WLAN works in centralized forwarding mode.
- Run the **tunnel local** command in WLAN configuration mode to set the WLAN to the local forwarding mode.

Enabling the RIPT Function

- Mandatory configuration.
- Run the **ript enable** command to enable RIPT in AP/AP group configuration mode.
- Enabling the RIPT function on an AP does not affect existing services when the AP is normally connected to the AC.

Command	**ript enable**
Parameter Description	N/A
Defaults	The RIPT function is disabled.
Command Mode	AP configuration mode/ AP group configuration mode
Configuration Usage	N/A

Enabling or Disabling the AC Configuration Change Monitoring Function

- Optional configuration.

Command	**ript-monitor** { **enable** | **disable** }
Parameter Description	**enable**: Enables the AC configuration change monitoring function. **disable**: Disables the AC configuration change monitoring function.
Defaults	The AC configuration change monitoring function is enabled.
Command Mode	Privileged EXEC mode or global configuration mode
Configuration Usage	N/A

Enabling SSID After Connection Interruption

- Optional
- Perform this operation in WLAN configuration mode.
- If the RIPT function is not enabled for the AP, this function does not take effect. After the AP connection is interrupted, SSID signals are not provided.
- Run the **enable-ssid at-capwap-down** command in WLAN configuration mode to enable SSID after connection interruption.

Command	enable-ssid at-capwap-down
Parameter Description	N/A
Defaults	By default, the function of SSID enabling after connection interruption is disabled.
Command Mode	WLAN configuration mode
Usage Guide	This function needs to be enabled only if 802.1X authentication is used.

Enabling Free Web Authentication After Connection Interruption

- Optional
- Perform this operation in WLAN configuration mode.
- Free Web authentication after connection interruption is performed only after this function is enabled on WLANs adopting web or MAB authentication.

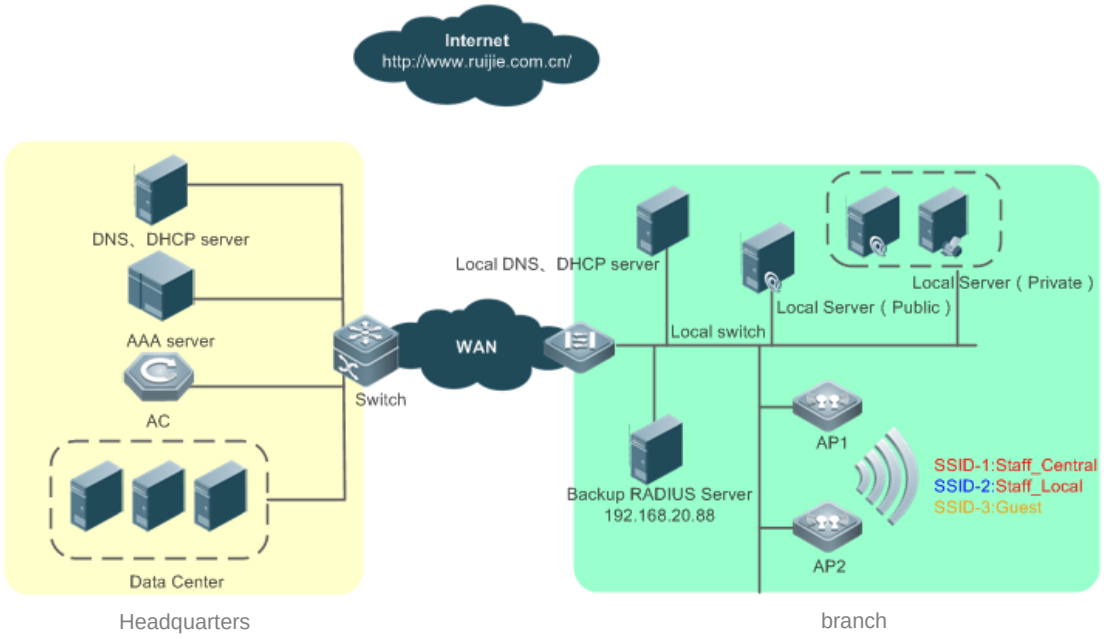
Command	free-webauth at-capwap-down
Parameter Description	N/A
Defaults	By default, free web authentication after connection interruption is disabled.
Command Mode	WLAN configuration mode
Usage Guide	This function needs to be enabled only on WLANs adopting Web or MAB authentication.

Verification

- Run the **show ap-config summary ript-enable** command to check whether the RIPT function is enabled on the AP.
- Run the **show running-config** command to check whether the functions of SSID enabling after connection interruption and free Web authentication after connection interruption are enabled.
- When the AC is normally connected, STAs can normally get online. When the AC is restarted or disconnected, online STAs can maintain normal communications and new STAs can normally access the network.
- For WLANs with the function of SSID enabling after connection interruption enabled, SSID signals are provided only after the AP connection is interrupted.
- For WLANs enabling web authentication and free Web authentication after connection interruption, STAs can access the network without web authentication only after the AP connection is interrupted.

Configuration Steps

Configuring the RIPT Function

Scenario **Figure 3-3**	
Configuration Steps	● Create a WLAN, and set it to the local forwarding mode and. ● Configure an AP group, specify WLAN mapping for the AP group. ● Configure the APs, add them to the AP group, and enable the RIPT function on the APs. ● For 802.1X authentication, enable the function of SSID enabling after connection interruption. ● For Web authentication, enable free Web authentication after connection interruption.

AC	Ruijie# configure terminal Ruijie(config)# vlan 106 Ruijie(config-vlan)# exit Ruijie(config)# vlan 107 Ruijie(config-vlan)# exit Ruijie(config)# wlan-config 1 Staff Ruijie(config-wlan)# tunnel local Ruijie(config-wlan)# exit Ruijie(config)# wlan-config 2 Staff_local Ruijie(config-wlan)# tunnel local Ruijie(config-wlan)# exit Ruijie(config)# wlan-config 3 guest Ruijie(config-wlan)# tunnel local Ruijie(config-waln)# free-webauth at-capwap-down Ruijie(config-wlan)# exit Ruijie(config)# wlan-config 20 Staff-1x-esc Ruijie(config-wlan)# tunnel local Ruijie(config-wlan)# enable-ssid at-capwap-down Ruijie(config)# ap-group apg-test Ruijie(config-ap-group)# interface-mapping 1 106 ap-wlan-id 1 Ruijie(config-ap-group)# interface-mapping 2 106 ap-wlan-id 2 Ruijie(config-ap-group)# interface-mapping 3 107 ap-wlan-id 3 Ruijie(config-ap-group)# interface-mapping 20 107 ap-wlan-id 4 Ruijie(config-ap-group)# exit Ruijie(config)# ap-config AP1 Ruijie(config-ap)# ap-group apg-test Ruijie(config-ap)# ript enable Ruijie(config-ap)# exit Ruijie(config)# ap-config AP2 Ruijie(config-ap)# ap-group apg-test Ruijie(config-ap)# ript enable Ruijie(config-ap)# end
Verification	Run the **show ap-config summary ript-enable** command to display the RIPT status of the APs. Run the **show running-config** command to display the configuration.

AC

```
Ruijie# show ap-config summary ript-enable
AP Name                                  IP Address      Mac Address    ript-enable State
---------------------------------------- --------------- -------------- ----------- -----
AP1                                      172.18.18.11    001a.0000.de47 Y           Run
AP2                                      172.18.18.12    001a.0000.de48 Y           Run
Ruijie# show running-config
…
!
wlan-config 1 Staff
 tunnel local
!
wlan-config 2 Staff_local
 tunnel local
!
wlan-config 3 guest
 tunnel local
 free-webauth at-capwap-down
!
wlan-config 20 Staff-1x-esc
 tunnel local
 enable-ssid at-capwap-down
!
…
```

Common Errors

N/A

3.5 Monitoring

Displaying

Function	Command
Displays the RIPT configuration of APs.	**show ap-config summary ript-enable**
Displays the AC monitoring configuration.	**show ript-monitor**

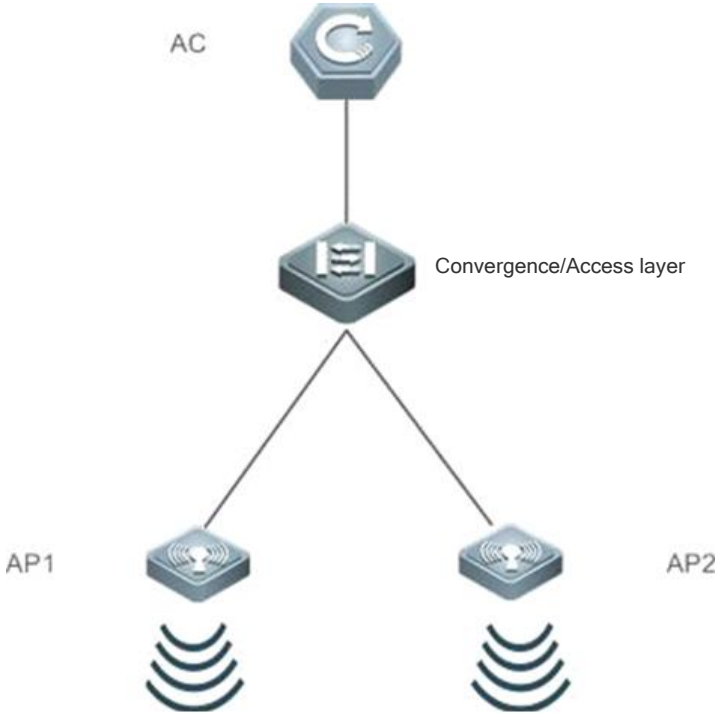
4 Configuring Virtual AC

4.1 Overview

In an AC+fit AP distributed network, there are thousands of and even tens of thousands of APs. How to guarantee reliability of wireless access is essential in a large-scale network.

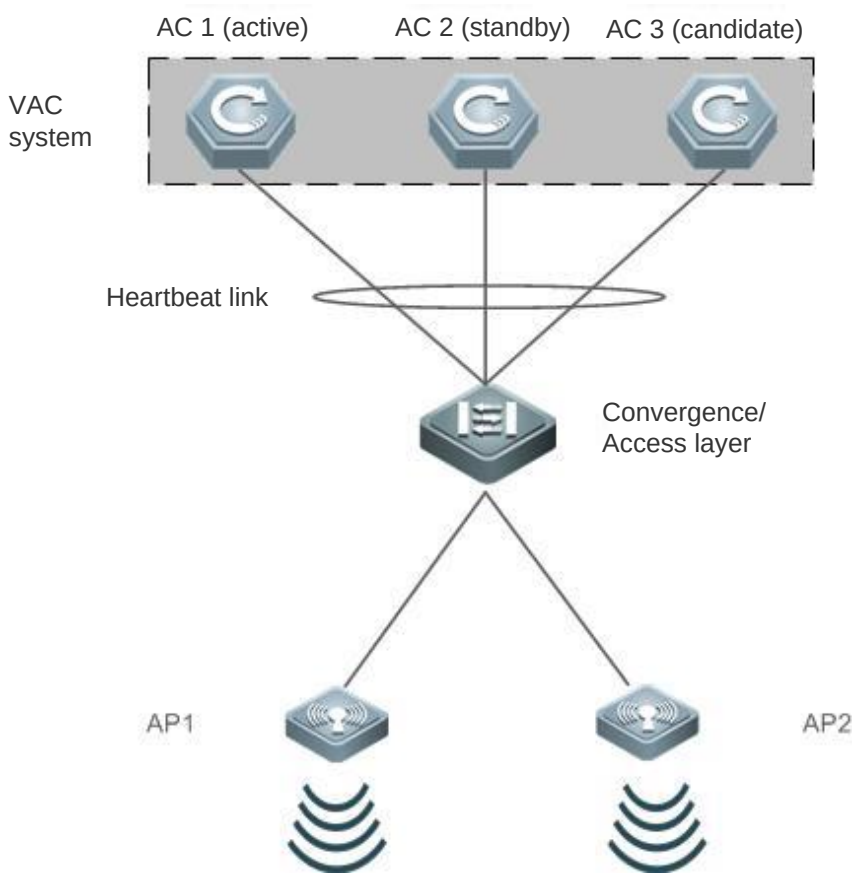
In existing AC+fit AP networking mode, an AP discovers the AC via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. The AP can receive services from the AC only after being successfully registered and associated with the AC. As a result, the process in which an AP detects whether the AC is faulty via CAPWAP keepalive packets is very time-consuming. If an AC malfunctions, all APs need to re-register with another AC. The incurred network interruption duration imposes great impact on enterprises. How to shorten the switch time to reduce impact on the network is an issue to be urgently resolved.

Figure 4-1 Conventional Network Structure



Virtual AC (VAC) is a network system virtualization technology capable of combining multiple ACs into one virtual device. As shown in Figure 4-2, multiple ACs of the same model can form a VAC system. In comparison with the conventional networking mode, this networking simplifies the network topology, reduces network management and maintenance costs, shortens the application recovery time and service interruption time, and improves network resource utilization.

Figure 4-2 VAC Networking Mode



4.2 Applications

Application	Description
Managing Multiple Devices in Unified Manner	Multiple physical devices compose one logical device for unified management.
Improving the Reliability	Multiple devices are available for fast switching, thereby improving the reliability.

4.2.1 Managing Multiple Devices in Unified Manner

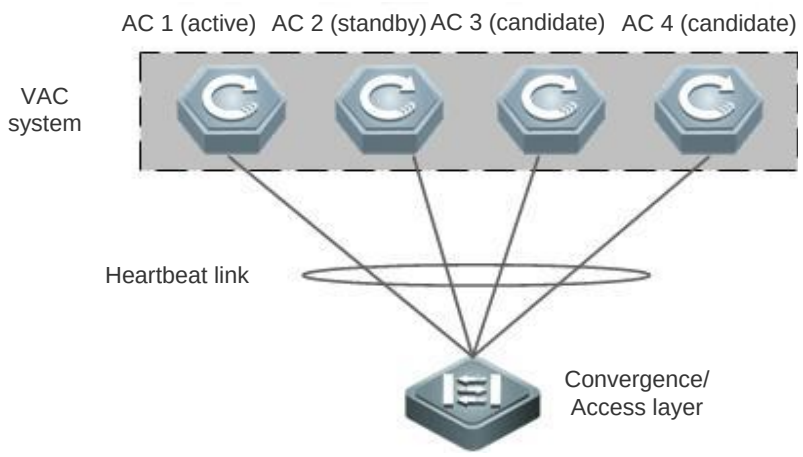
Scenario

When multiple physical devices compose a VAC system, the VAC system can be considered as one logical device. All configurations are managed on the global active device.

As shown in Figure 4-3, four devices (numbered 1, 2, 3, and 4 from left to right in sequence) compose a VAC system. Device 1 is the global active device, Device 2 is the global standby device, and Device 3 and Device 4 are global candidate devices.

- Configurations only need to be performed on the active device for device management.

Figure 4-3



Remarks	The devices are numbered 1, 2, 3, and 4 from left to right in the figure above. For the heartbeat link, see descriptions in section 1.3.1. Device 1 serves as the global active device. Device 2 serves as the global standby device. Device 3 and Device 4 serve as the global candidate devices.

Deployment

- The active device is responsible for controlling the entire VAC system, running the management plane protocols, running the control plane protocols of the active device, and participating in data forwarding.
- The standby device is responsible for running the control plane protocols of the standby device, participating in data forwarding, and taking over the work of the active device when the active device malfunctions.
- Global candidate devices are responsible for running the control plane protocols of the candidate devices and participating in data forwarding. When the global standby device malfunctions, a global candidate device can take over the work of the global standby device and serves as the global standby device. A global candidate device cannot take over the work of the global active device. Therefore, when the global active device and the global standby device malfunction at the same time, the VAC system restarts.
- Control plane protocols are mutually backed up among the devices.

4.2.2 Improving the Reliability

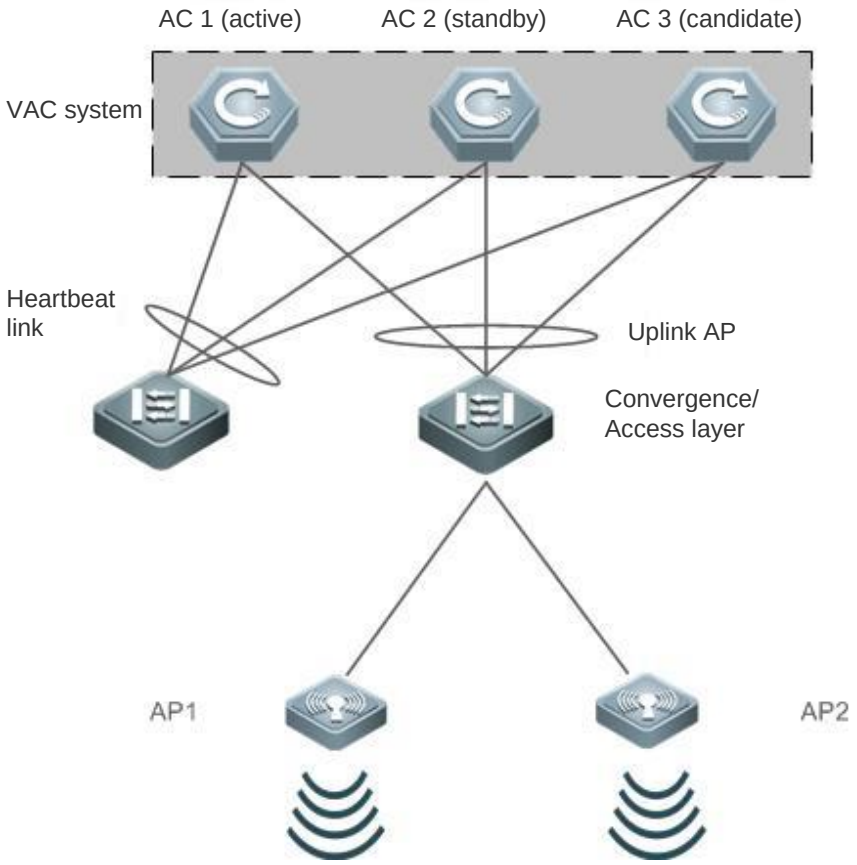
Scenario

As shown in Figure 4-4, when the AC malfunctions, all APs registered with the AC drop out of the network. The APs need to rediscover another AC and complete the registration so as to reconnect to the network. All devices in a VAC system are considered as one logical device. A device in the VAC system mutually serves as a backup of other devices. When one device malfunctions, services and data can be rapidly migrated to another device.

- Multiple ACs form a VAC system and the ACs provide mutual redundancy. System management is conducted on the active device.

- A heartbeat link is configured between ACs to provide a data channel and exchange data. ACs are connected to the access/convergence layer through the uplink AP.
- When one device in a VAC system malfunctions, other devices work properly.

Figure 4-4



Deployment

- The active device is responsible for managing the entire VAC system, running the management plane protocols, running the control plane protocols of the active device, and participating in data forwarding.
- The global standby device is responsible for participating in data forwarding, running the control plane protocols but not the management plane protocols, and taking over the work of the global active device when the global active device malfunctions.
- The heartbeat link occupies an independent port on the AC, and services are not configured on the port.

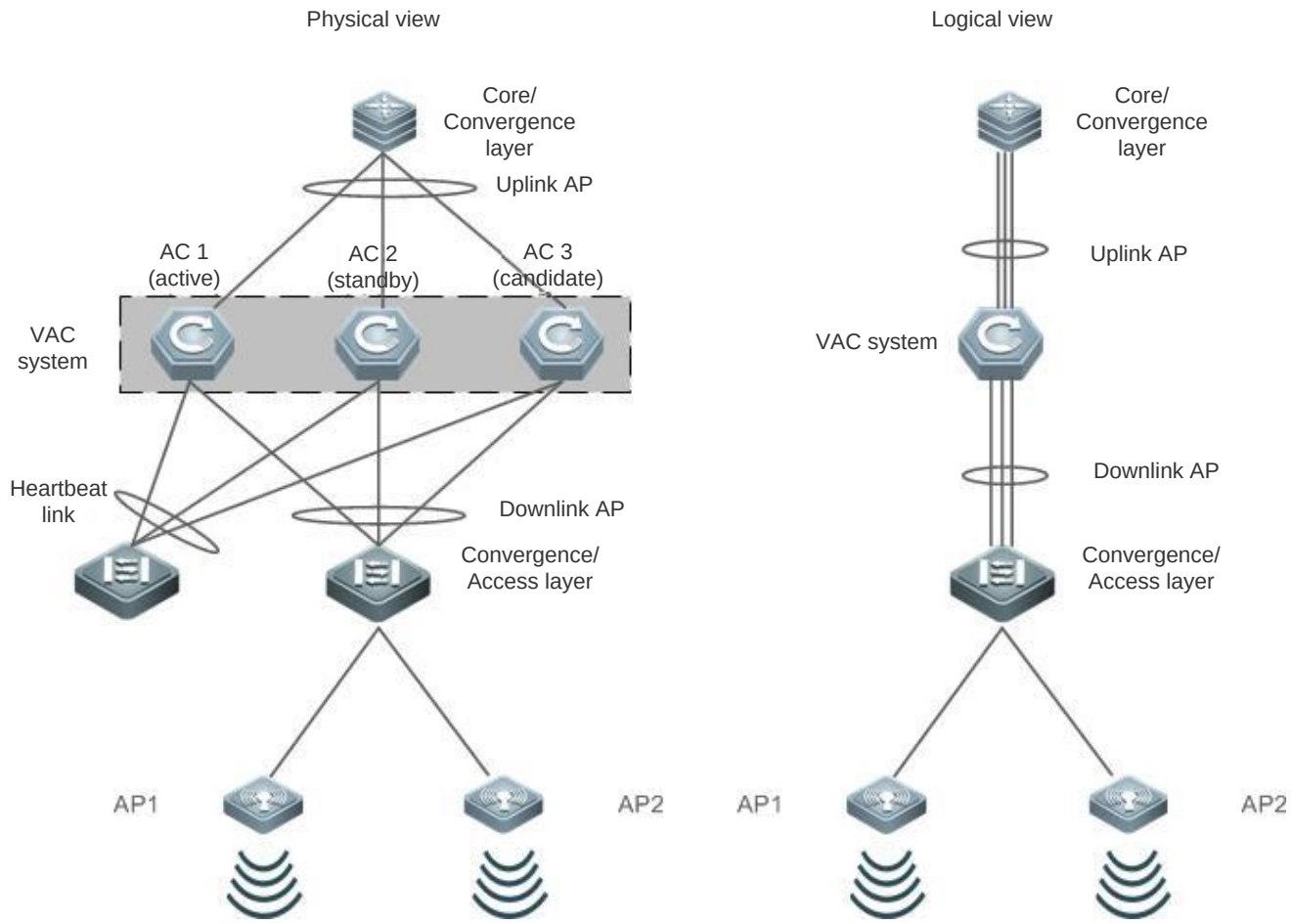
4.3 Features

Basic Concepts

VAC System

A VAC system is a single logical entity composed of multiple independent ACs in the conventional network structure that are connected through internal heartbeat links. A VAC system can be considered as an independent AC for management.

Figure 4-5 VAC System



Domain ID

A VAC system has a unique domain ID. Only devices with the same domain ID can form a VAC system.

Device ID

Each member device in a VAC system has a unique device ID. This device ID facilitates management on member devices. When adding a device to a VAC system, you need to configure a device ID for the device and ensure that the device ID is unique in the VAC system. If device IDs of member devices conflict in a VAC system, one member device is retained according to the priority.

Device Role

When a VAC system is built, one device is elected as the active device, and another device is elected as the standby device according to the election protocol mechanism, the standby device and the rest devices serve as candidate devices. The

active device is responsible for controlling the entire VAC system, running the management plane protocols of the VAC system, running the control plane protocols of the active device, and participating in data forwarding. The standby device and candidate devices do not run management plane protocols, but run their respective control plane protocols and participate in data forwarding. When the active device fails, the standby device serves as the active device to manage the VAC system.

The active device of a VAC system is elected as follows:

1. The rules for active device election are as follows (if the active device cannot be elected according to the previous rule, the system goes on with the next rule for judgment): (a) The current running device is elected as the active device preferentially (No device is the active device during startup). (b) A member device with the highest priority is elected as the active device. (c) A member device with a smaller device ID is elected as the active device. (d) A member device with a smaller MAC address is elected as the active device.
2. The VAC system supports the joining of a device in hot mode. The system does not perform active/standby switching even if a device that joins the VAC system in hot mode has a higher priority than the active device in the VAC system.
3. The startup sequence of member devices may affect election of the active device. Some member devices may not join the VAC system in time due to slow startup (currently, the VAC system directly conducts convergence if it does not discover a neighbor within 5 minutes). In this case, the member device will join the VAC system in hot mode. Even if its priority is higher than the current running active device in the VAC system, the system does not perform active/standby switching.

Overview

Feature	Description
Heartbeat Link	Describes relevant features of the heartbeat link of the VAC system.
Topology	Describes the topology structure of the VAC system.
Dual-Active Detection	Prevents the coexistence of dual active devices in the same VAC system domain.
External Connections of Devices in the VAC System	Describes the connections between external devices and devices in the VAC system.
System Management	Manages devices in the VAC system.

4.3.1 Heartbeat Link

Working Principle

Heartbeat Link

The active and standby devices in a VAC system are network entities and they need to transmit management information to each other. Heartbeat links are special links for transmitting management information (including role election information and configuration backup information) and data streams between devices in the VAC system. Users can configure one or more heartbeat links between two member devices of a VAC system. Two heartbeat links are recommended for scenarios with high reliability requirements.

After the VAC system is established, if one heartbeat link fails, the VAC system automatically adjusts the configuration so that the backup traffic is not transmitted via the failed link.

If all heartbeat links are disconnected, the topology of the VAC system is split, and the standby device automatically becomes the active device. The configurations of the two devices are the same, which will trigger dual-active detection. One of the two active devices will enter the recovery state and the service port on the device is disabled, so as avoid impact on services in the user network.

If the active device malfunctions, the standby device can detect the fault of the active device via the heartbeat link, automatically becomes the active device, and takes over services.

Heartbeat links can be directly connected or connected through a Layer-2 switch.

Heartbeat Link Traffic

Data streams transmitted by heartbeat links between devices are classified into the following:

- Flooding data streams in a VLAN
- Data streams to be forwarded between devices, which need to be transmitted via heartbeat links.

In addition, heartbeat links also transmit internal management packets of the VAC system, for example, hot backup control plane protocol information, and packets that carry the configuration to be delivered from the active device to other member devices.

4.3.2 Topology

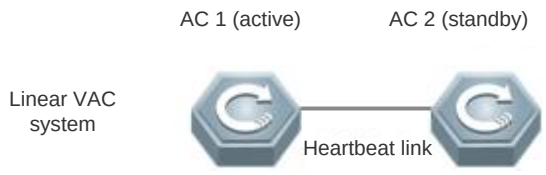
The VAC system supports the linear topology structure and star topology structure. Devices are connected through a heartbeat link, which can be considered as a line and this topology is called linear topology. Multiple ACs are connected through a Layer-2 switch and the topology in this structure is called star topology.

Working Principle

Topology Structure

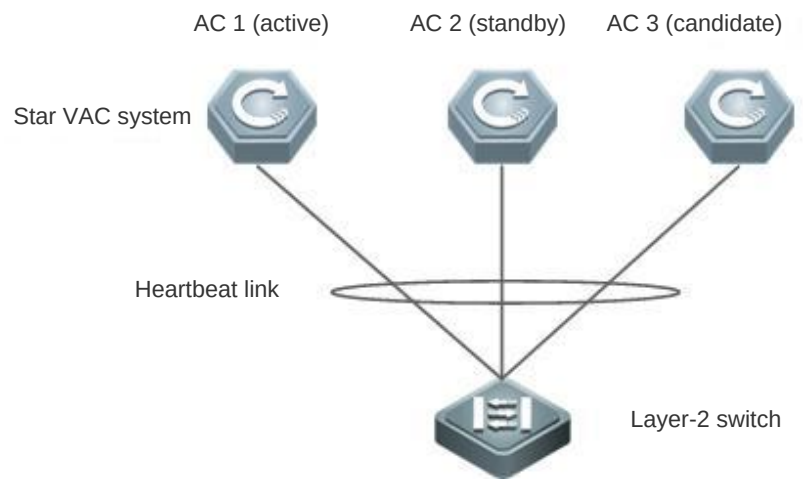
In the linear topology, ACs are directly connected via a heartbeat link. Currently, a linear VAC system can be composed of only two devices. A VAC system consisting of three or more devices must use the star topology.

Figure 4-6 Linear Topology



As shown in Figure 4-7, ACs can be connected through a Layer-2 switch to form a star topology. This topology reduces the number of the ports occupied by heartbeat links.

Figure 4-7 Star Topology



Topology Election

Before a VAC system is established, member devices discover their neighbors via the topology discovery protocol, to determine the devices that compose the VAC system, so as to determine the scope of the management domain. Then, one active device is elected to manage the VAC system and one standby device is elected as the backup of the active device. At this point, the topology of the VAC system is converged. The topology discovery protocol information is transmitted via heartbeat links. The startup time of different devices is different. Therefore, the first convergence time of the topology is different.

The rules for active device election are as follows (active device election starts from the first rule; if the active device is not elected according to the current rule, the system goes on with the next rule for judgment):

- Topology convergence status. The device whose topology is converged is elected as the active device preferentially.
- Priority. The device with a higher priority is elected as the active device.
- If the active device cannot be determined according to the preceding rules, the device with a smaller device ID will prevail.
- If the active device cannot be determined according to the preceding rules, the device with a smaller MAC address will prevail.

The rules for standby device election are as follows (standby device election starts from the first rule; if the standby device is not elected according to the current rule, the system goes on with the next rule for judgment):

- Compare with the ID of the switch connected to the active device. The device that does not reside on the same switch as the active device is preferentially elected as the standby device. If multiple devices are not on the same switch as the active device, go on with the next rule for judgment.
- Priority. The device with a higher priority is elected as the standby device.
- If the standby device cannot be determined according to the preceding rules, the device with a smaller device ID will prevail.

- If the standby device cannot be determined according to the preceding rules, the device with a smaller MAC address will prevail.

Topology Combination

When two or more ACs with the same domain ID are connected via heartbeat links, the topologies will be combined. One device will restart and join the VAC system in hot mode during topology combination.

The topology combination rules are as follows (the topology combination starts from the first rule. If the optimal topology is not selected according to the first rule, the system goes on with the next rule for judgment):

- The user configuration is prior to other configuration. The device configured with the highest priority will prevail.
- If the active device cannot be determined according to the preceding rule, the device with a smaller device ID will prevail.
- If the active device cannot be determined according to the preceding rule, the device with a smaller MAC address will prevail.

Heartbeat Link Passing Through a Layer-2 Network

In a star topology environment, heartbeat links are not directly connected, and a Layer-2 switch is used to forward management packets carried over the heartbeat links. In a VAC system, management packets of devices cannot be forwarded across VLANs. Therefore, on the Layer-2 switch, heartbeat link ports of multiple ACs must be configured to be in the same VLAN. It is recommended to configure a separate VLAN for AC heartbeat link ports on the switch, so as to prevent other ports in the same VLAN from interfering with management packet forwarding.

4.3.3 Dual-Active Detection

Working Principle

When the heartbeat link is disconnected, the standby device becomes the active device. If the original active device is still running, there are two active devices and IP address conflict and other problems will be incurred in the LAN because they have the same configuration. In this case, the VAC system must detect whether dual active devices coexist, and take recovery measures.

Rules of Dual-Active Detection

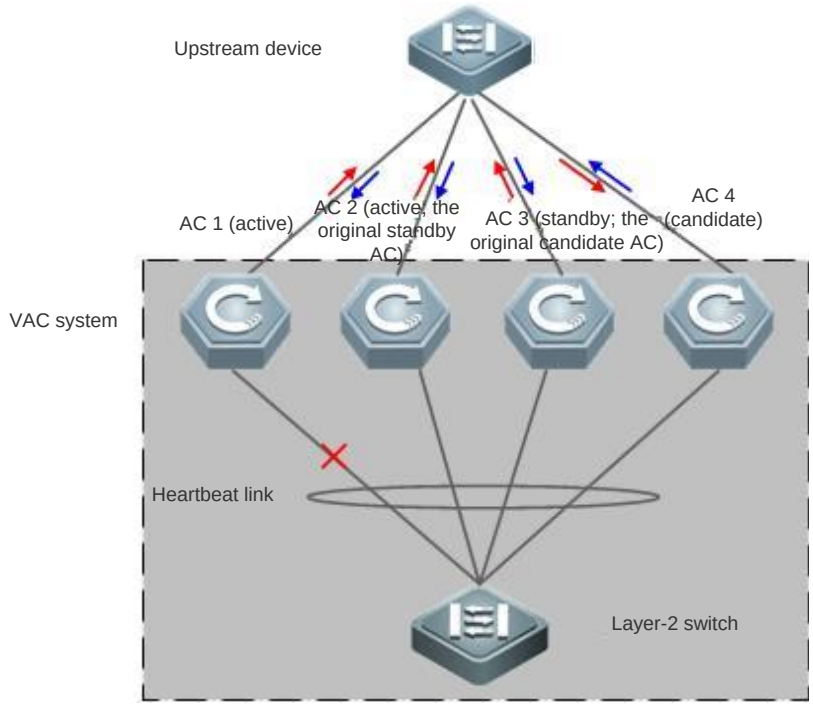
1. The device with a higher priority will prevail.
2. If the active device cannot be determined according to the preceding rule, the device with a smaller device ID will prevail.
3. If the active device cannot be determined according to the preceding rules, the device with a smaller MAC address will be retained.
4. If the active device cannot be determined according to the preceding rules, the device with longer startup time will be retained.


If dual-active detection is not configured, the network will be interrupted after the topology is split.

Dual-Active Detection Mode

The VAC system supports the dual-active detection mechanism by using an aggregate port. Figure 4-8 shows the connection topology. Both the VAC system and upstream device need to support the dual-active detection function of the aggregate port. When a heartbeat link is disconnected and dual active devices coexist, both active devices send inspection packets to each member port of the aggregate port. The inspection packets are transferred by the upstream device to the other active device. As shown in Figure 4-8, the aggregate port contains four member ports, each of which is connected to one device in the VAC system. When the topology is split, the four member ports send and receive inspection packets to detect the coexistence of dual active devices. Then, according to certain rules (same as topology combination rules), the VAC system where one active device resides will be shut down to enter the recovery state, so as to prevent network abnormalities.

Figure 4-8 Dual-Active Detection



4.3.4 Traffic Forwarding

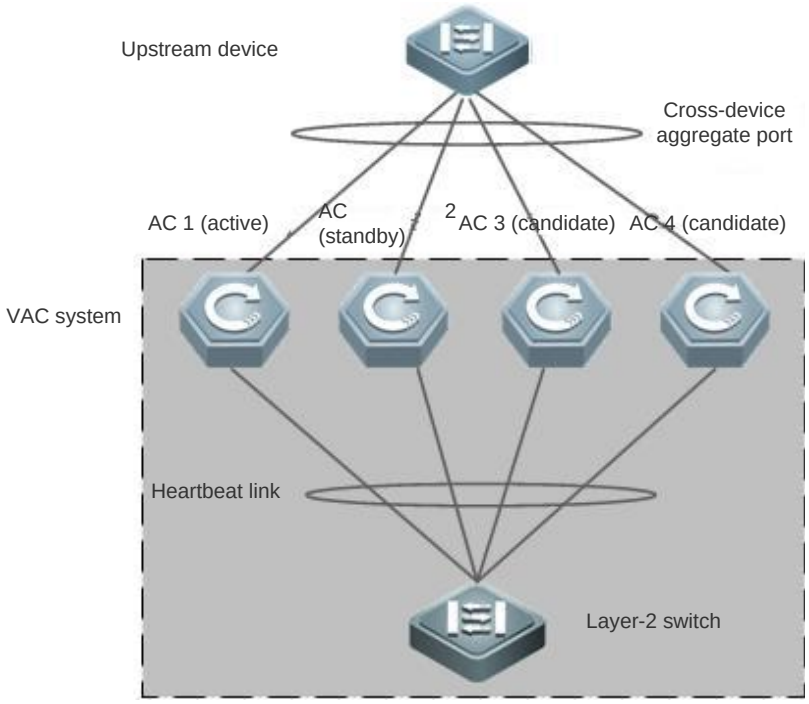
Working Principle

Cross-device Aggregate Port Group

An AP binds multiple physical connections to form a logical connection. The VAC system supports the AP across member devices.

As shown in Figure 4-9, four ACs compose the VAC system and the upstream device is connected to the VAC system as an AP. For the upstream device, the AP connections are equivalent to a common aggregate port group.

Figure 4-9 Cross-device Aggregate Port



Troubleshooting

It is recommended that a peripheral device be physically connected to each device in the VAC system when a cross-device AP is configured for the VAC system. This can ensure the bandwidth of heartbeat links on one hand (the cross-device AP preferentially selects the AP member port as the traffic outlet, to prevent transmission of unnecessary traffic via heartbeat links), and improve the network reliability on the other hand (if a device malfunctions, member ports on the normal devices can work properly).

The possible cross-device AP failures and incurred impact are described as follows:

- A single link fails.

If a single link of the cross-device AP fails but other links function properly, the cross-device AP re-distributes traffic among the remaining normal links.

- On the global active device, links of all cross-device AP member ports fail.

If links of all cross-device AP member ports on the global active device fail, only member ports on other member devices continue to work properly. If the forwarding egress port of data streams coming from the AP to the VAC system is located on the global active device, the VAC system forwards the data streams to the egress port of the global active device via heartbeat links.

Control plane protocols run on each device. Therefore, protocol packets transmitted to the VAC system are forwarded to each device for protocol computing via the heartbeat links.

- All links to other member devices fail.

If all links between the cross-device AP and Member Device A fail, only member ports on other member devices continue to work properly. If the forwarding egress port of data streams coming from the AP to the VAC system is located on Member Device A, the VAC system forwards the data streams to the egress port of Member Device A via heartbeat links.

- All links fail.

If all links of the cross-device AP fail, the cross-device AP changes the port state to Link-Down, just as a common AP does.

- The global active device malfunctions.

If the active device malfunctions, hot backup switching is triggered and the original standby device becomes the active device. Meanwhile, member ports on other member devices continue to work properly. When the peer device in the VAC system that is connected to the cross-device AP detects a link failure, it adjusts the load balancing algorithm to distribute data streams to normal links.

- A member device malfunctions.

If a member device malfunctions, the AP member ink connected to the member device is disconnected but other member links still work properly. When the peer device in the VAC system that is connected to the cross-device AP detects a link failure, it adjusts the traffic balancing algorithm to distribute data streams to normal links.

Traffic Balancing

There may multiple traffic egresses in a VAC system. The AP and Equal-cost Multi-path Routing (ECMP) have their own traffic balancing algorithms, for example, traffic is balanced based on the source and destination MAC addresses. For details, see the AP and ECMP configuration manuals. In this configuration manual, packets received by the local device can be configured to be preferentially forwarded by the local device. In this way, packets can be forwarded to other devices not through heartbeat links.

4.3.5 System Management

Working Principle

Console Access

The console of the active device in the VAC system is also used to manage multiple devices in the system. On the console of the standby device, CLI commands cannot be executed, but the protocol status of the standby device can be queried and protocol entries can be cleared. On the active device, users can configure services for member devices in a unified manner. Users can also log in to the console of the active device through the serial port of the standby device. In addition, users can redirect to the console of a device by running run the **session** command.

Interface Naming

In VAC system work mode, the same port ID may appear on multiple devices. Therefore, the device ID is introduced to interface naming.

For example, interface gigabitEthernet 1/0/1 indicates the GE Port 1 in Slot 0 of the device with the ID of 1; interface gigabitEthernet 2/0/2 indicates the GE Port 2 in Slot 0 of the device with the ID of 2.

System Upgrade

Usually, the main program versions of member devices in the VAC system need to be consistent. However, there are numerous member devices and the upgrade is time-consuming, laborsome, and error-prone if the devices are upgraded in standalone mode. Currently, a perfect system upgrade solution is available. You can complete the system upgrade by using the two methods below:

- When the VAC system is established, the system automatically checks the main program version of all member devices. If inconsistency is identified, the system synchronizes the main program of the active device to all member devices.
- After the VAC system is established, the system automatically synchronizes the file downloaded over TFTP to all member devices.

System Logs

System logs can be printed on all member ports of the VAC system. System logs generated by the active device are directly printed on the console of the active device, and the format of printed system logs is identical to that of system logs printed in standalone mode. System logs generated by other member devices are also printed on the console of the active device, but the format of printed system logs is different from that of system logs printed in standalone mode because the device ID is printed.

For example, the system log generated in standalone mode is "%DEVICE-6-INSTALL: Install chassis WS5708 on device 1." The system log generated by the member device with the device ID of 2 should be "%DEVICE-6-INSTALL: (2*)Install chassis WS5708 on device 1.

4.3.6 Standby Device Preemption

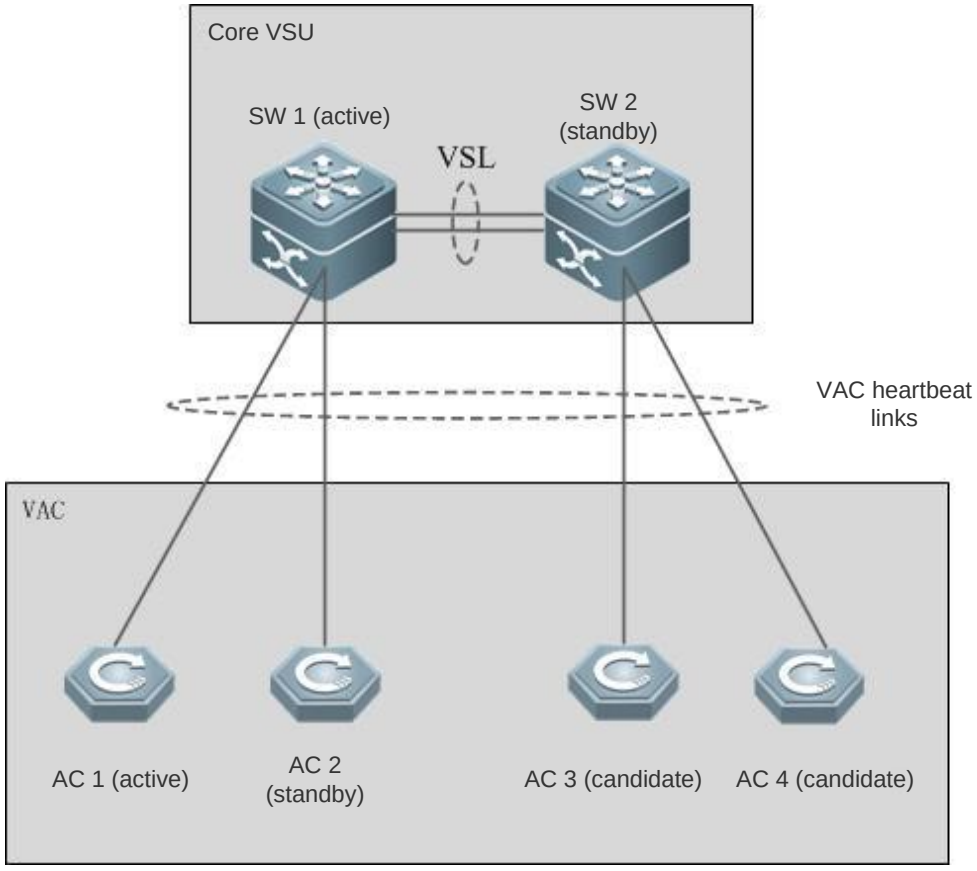
Working Principle

Standby Device Preemption

The VAC system supports the standby device preemption function. If a new device that joins the VAC system has a higher priority than the existing standby device in the VAC system, the new device will preempt the standby device role.

As shown in Figure 4-10, SW 1 and SW 2 compose a VSU, ACs 1-4 are connected to the two switches and form a VAC system. The active and standby devices of the VAC system connect to SW 1 and the candidate ACs are connected to SW 2.

Figure 4-10 VSU+VAC



When the core VSU malfunctions, SW 1 resets, which will result in splitting of the VAC system. AC 1 and AC 2 cannot communicate with external devices, resulting in the AP drop-out. AC 3 and AC 4 have no standby devices and will reset for recovery upon splitting. Therefore, when one switch in the VSU malfunctions, all ACs will become unavailable, which is contradictory to the original intention of the VAC system, and backup cannot be performed correctly.

The standby device preemption function can properly solve this problem. ACs with high priority are connected to different switches. In this way, the active and standby devices in the VAC system are connected to different switches. When the VSU malfunctions, one switch resets, ACs connected to the other switch can take over services properly, preventing unavailability of all ACs.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic VAC System Parameters in Standalone Mode	⚠ (Mandatory) It is used to configure VAC system parameters in standalone mode.	
	virtual-ac domain	Configures the domain ID.
	device	Configures the device ID in the VAC system.

		device priority	Configures the device priority.
		device connect_switch	Configures the ID of the switch connected to the AC.
		vac-port	Enters the heartbeat port configuration mode.
		port-member interface	Adds a common port to the heartbeat link port pool.
		device convert mode vitual	Switches the device from the standalone mode to the VAC mode.
Configuring VAC System Parameters in VAC Mode	Configuring VAC System Attributes	⚠ (Optional) It is used to configure device attributes in VAC mode.	
		device domain	Changes the domain ID of the device.
		device renumber	Changes the device ID.
		device description	Configures the device alias.
	Configuring Heartbeat Links	⚠ (Optional) It is used to configure heartbeat links.	
		vac-port	Enters the heartbeat port configuration mode.
		port-member interface	Adds a common port to the heartbeat link port pool.
	Configuring Dual-Active Detection	⚠ (Mandatory) It is used to configure the dual-active detection function.	
		dual-active detection	Configures the dual-active detection function.
		dual-active bfd interface	Configures a BFD detection port.
		dual-active interface	Configures the aggregate port as the dual-active detection port.
		dual-active exclude interface	Configures an excluded port.
	Configuring Standby Device Preemption	**slave preemtive enable**	Configures standby device preemption.
	Switching the Device from VAC Mode to Standalone Mode	⚠ (Optional) It is used to switch the device from the VAC mode to the standalone mode.	
		device convert mode standalone	Switches the device from the VAC mode to the standalone mode.
Monitoring	Displaying Current Running Status	⚠ Optional.	
		show virtual-ac	Displays information about the currently running VAC system, topology structure, or current VAC system parameters.

		show virtual-ac dual-active	Displays the current dual-active detection configuration.
		show virtual-ac link	Displays the heartbeat link running status in VAC mode.
		session	Redirects to the console of the active device or any device.

4.4.1 Configuring Basic VAC System Parameters in Standalone Mode

Configuration Effect

Configure VAC-relevant basic parameters, so as to build a VAC system.

Configuration Steps

Configuring VAC System Attributes

- Configure the same domain ID for multiple devices that need to compose a VAC system and ensure that the domain ID is unique in the LAN. In addition, configure a device ID for each device in the VAC system.
- Run the **vitrual-ac domain** *domain_id* command to configure the domain ID. This command is mandatory.
- Run the **device** device_*id* command to configure a device ID for each device in the VAC system. This command is mandatory. When devices share the same priority, the device with a smaller device ID is preferentially elected as the primary device.
- Run the **device** *device_id* **priority** *priority_num* command to configure the device priority. This command is optional. The value ranges from 1 to 255. A larger value indicates a higher priority.

Command	**virtual-ac domain** *number*
Parameter Description	*number*: Indicates the virtual domain ID of a VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only devices with the same domain ID can compose a VAC system. The domain ID must be unique in the LAN.

Command	**device** *device_id*
Parameter Description	*device_id*: Indicates the ID of a device in the VAC system. The value varies with the product model.
Defaults	The default device ID is 1.
Command Mode	config-vac-domain configuration mode

Usage Guide	The device with a smaller device ID is elected as the active device if two devices are both active devices or if the two devices share the same priority and are just started with their roles not determined. This command can be used to change the ID of an AC only in standalone mode. The changed device ID takes effect only after device restart.

Command	**device** *device_id* **connect_switch** *switch_id*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. *switch_id*: Indicates the device ID. The value ranges from 1 to 255.
Defaults	The default switch ID is 1.
Command Mode	config-vac-domain configuration mode
Usage Guide	Set the ID of the connected switch. If the specified switch ID is different from that of the active device, the device will be preferentially elected as the standby device. This command is available in both the standalone mode and VAC mode. The changed priority takes effect only after the device restart. In VAC mode, *device_id* indicates the ID of the currently running device. If the device ID does not exist, the priority configuration does not take effect.

Command	**device** *device_id* **priority** *priority_num*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. priority_num: Indicates the device priority. The value ranges from 1 to 255.
Defaults	The default priority is 100.
Configuration Mode	config-vac-domain configuration mode
Usage Guide	A larger value indicates a higher priority. The device with a higher priority is elected as the active device. This command is available in both the standalone mode and VAC mode. The changed priority takes effect only after device restart. In VAC mode, *device_id* indicates the ID of the currently running device. If the device ID does not exist, the configuration does not take effect.

The priority configuration command is used to change the priority only and will not change the device ID. Therefore, a correct device ID must be entered during configuration. For example, the configured device ID is 1. If you enter the **device 2 priority 100** command, the priority does not take effect.

Configuring Heartbeat Links

- Some ports need to be configured as heartbeat detection ports so as to establish a VAC system.
- Run the **vac-port** command to enter the heartbeat port configuration mode. This command is mandatory.
- Run the **port-member interface** *interface-name* [**copper** | **fiber**] command to add heartbeat ports. This command is mandatory.

- When the device enters the heartbeat port configuration mode, you can configure or delete heartbeat ports.

Command	**vac-port**
Parameter Description	N/A
Defaults	N/A
Command Mode	Configuration mode
Usage Guide	This command is available in both the standalone mode and VAC mode.

Command	**port-member interface** *interface-name* [**copper | fiber**]
Parameter Description	*interface-name*: Indicates a 2D port name, for example, Tengigabitethernet 1/1 and Tengigabitethernet 1/3. **copper**: Indicates the electrical port attribute. **fiber**: Indicates the SFP port attribute.
Defaults	*N/A*
Command Mode	config-vac -port configuration mode
Usage Guide	Add member ports for the heartbeat links. *interface-name* indicates the 2D port name in standalone mode. It can be a 10GE port or a GE port (the GE port can be an SFP combo port. If the medium type is not specified, the GE port is a GE electrical port by default). The optical/electrical attribute must be specified for SFP combo ports. This command is available in both VAC mode and standalone mode.

⚠ In standalone mode, the heartbeat port configuration does not take effect immediately. It can take effect only after the device switches to VAC mode and is restarted.

Verification

Run the **show virtual-ac config** [*device_id*] command to display the VAC system configuration on the current device in standalone mode.

Command	**show virtual-ac config [** *device_id* **]**
Parameter Description	*device_id*: Indicates the device ID. If this parameter is specified, only the VAC system configuration of a specific device is displayed.
Command Mode	Privileged EXEC mode
Usage Guide	Display the VAC system configuration in standalone mode or VAC mode.

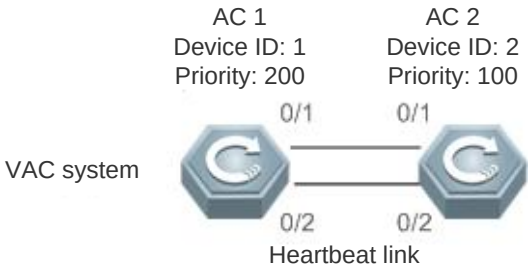
⚠ The VAC-relevant configuration is applicable to a single physical device, and the configuration is stored in the special configuration file **config_vac.dat**. Therefore, the **show running config** command cannot display VAC system

configuration. Only the **show virtual-ac** config command can be executed to display the configuration of the current VAC system.

In standalone mode, the running information of the VAC system is blank. When the **show virtual-ac** command is executed, a prompt is displayed, indicating that the current work mode is standalone mode and there is no VAC system running information.

Configuration Example

Configuration Example

Scenario **Figure 4-11**	 AC 1 and AC 2 form a VAC system. The domain ID is 100. The device ID and priority of AC 1 are 1 and 200 respectively. Ports 0/1 and 0/2 are heartbeat ports. The device ID and priority of AC 2 are 2 and 100 respectively. Ports 0/1 and 0/2 are heartbeat ports.
Configuration Steps	1) Complete the following configuration on AC 1: ● Configure the VAC system attributes and heartbeat ports. ● Switch the device from the standalone mode to VAC mode. 2) Complete the following configuration on AC 2: ● Configure the VAC system attributes and heartbeat ports. ● Switch the device from the standalone mode to VAC mode.
Device-1	Ruijie# configure terminal Ruijie(config)# virtual-ac domain 100 Ruijie(config-vac-domain)#device 1 Ruijie(config-vac-domain)#device 1 priority 200 Ruijie(config-vac-domain))#exit Ruijie(config)# vac-port Ruijie(config-vac-port)#port-member interface GigabitEthernet 0/1 Ruijie(config-vac-port)#port-member interface GigabitEthernet 0/2 Ruijie(config)#exit
Device-2	Ruijie# configure terminal Ruijie(config)# virtual-ac domain 100 Ruijie(config-vac-domain)# device 2 Ruijie(config-vac-domain)# device 2 priority 200 Ruijie(config-vac-domain))#exit Ruijie(config)# vac-port

	Ruijie(config-vac-port)#port-member interface GigabitEthernet 0/1 Ruijie(config-vac-port)#port-member interface GigabitEthernet 0/2 Ruijie(config-vac-port)#exit
Verification	● Run the **show virtual-ac config** command to display the VAC system attributes of AC 1 and AC 2.
Device-1	Ruijie#show virtual-ac config device_id: 1 (mac: 1414.4b5b.54f8) ! virtual-ac domain 100 ! device 1 device 1 priority 200 ! device convert mode virtual ! port-member interface GigabitEthernet 0/1 ! port-member interface GigabitEthernet 0/2 !
Device-2	Ruijie#show virtual-ac config device_id: 2 (mac: 00d0.f822.33c0) ! virtual-ac domain 100 ! device 2 device 2 priority 100 ! device convert mode virtual ! port-member interface GigabitEthernet 0/1 ! port-member interface GigabitEthernet 0/2 !

4.4.2 Configuring VAC System Parameters in VAC Mode

4.4.2.1 Configuring VAC System Attributes

Configuration Effect

After devices compose a VAC system or when the VAC system is running, if some parameters need to be modified, you can log in to the console of the active device of the VAC system to modify parameters. You cannot enter global configuration mode from the console of the standby device.

Notes

- Configuration commands take effect only after the switch is restarted except the **device** *device_id* **description** *device*1 command, which takes effect immediately.

Configuration Steps

Entering the Domain Configuration Mode

- Optional.
- Run this command in VAC mode to enter the domain configuration mode. Only ACs with the same domain ID can form a VAC system. In VAC mode, you can change or configure a domain ID, device priority, and switch ID only after entering the domain configuration mode.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only two devices with the same domain ID can compose a virtual device. The domain ID must be unique in the LAN.

Changing the Domain ID of the VAC System

- Optional.
- To change the domain ID of a device, run this command on the console of the active device in the VAC system.

Command	**device** *device_id* **domain** *new_domain_id*
Parameter Description	*device_id*: Indicates the ID of the currently running device in VAC mode. The value varies with the product model. *new_domain_id*: Indicates the changed domain ID. The value ranges from 1 to 255.
Defaults	The default value is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available only in VAC mode and the configuration takes effect only after device restart.

Changing the Device ID

- Optional.
- To change the device ID of a device, run this command on the console of the active device in the VAC system.

Command	**device** *device_id* **renumber** *new_device_id*
Parameter Description	*device_id*: Indicates the ID of the currently running device in VAC mode. The value varies with the product model. *new_device_id*: Indicates the changed device ID.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available only in VAC mode and the configuration takes effect only after device restart. This command is used only to change the device ID and will not change configuration relevant to the device ID. In VAC mode, many configurations are relevant to the device ID (for example, the type of the device installed by running the **install** command, configuration commands in various interface modes, and configuration commands using the port ID). After the device ID is changed, check whether all configuration is correct.

Changing the Device Priority

- Optional.
- To change the priority of a device, run this command on the console of the active device in the VAC system.
- A larger value indicates a higher priority. The device with a higher priority is elected as the active device.

Command	**device** *device_id* **priority** *priority_num*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. *priority_num*: Indicates the device priority. The value ranges from 1 to 255.
Defaults	The default priority is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	A larger value indicates a higher priority. The device with a higher priority is elected as the active device. This command is available in both the standalone mode and VAC mode. The changed priority takes effect only after the device restart. This command will not change the device ID. In standalone mode, if *device_id* is set to 1 but the **device 2 priority 200** command is executed, the command does not take effect unless device_id is changed to 2 and the command is executed again. In VAC mode, *device_id* indicates the ID of the currently running device. If the device ID does not exist, the priority configuration does not take effect.

Configuring the Device Alias

- Optional.
- To configure an alias for a device, run this command on the console of the active device in the VAC system.
- Run the **device** device_*id* **description** *device1* command to configure the device alias. The device alias can contain a maximum of 32 characters.

Command	**device device**_*id* **description** *dev-name*
Parameter	*device_id*: Indicates the ID of the device with the priority to be configured.

Description	*dev_name*: Indicates the device name.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available in both the standalone mode and VAC mode. The configuration takes effect immediately in VAC mode.

Configuring the ID of the Switch Connected to a Device

- Optional.
- To configure the ID of the switch connected to a device, run this command on the console of the active device in the VAC system.
- Run the **device** *device_id* **connect_switch** *switch_id* command to configure the ID of the switch connected to a device. The value ranges from 1 to 255.

Command	**device** *device_id* **connect_switch** *switch_id*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. switch_id: Indicates the ID of the switch connected to the device.
Defaults	N/A
Command Mode	config-vac-domain configuration mode
Usage Guide	Set the ID of the connected switch. If the specified switch ID is different from that of the active device, the device will be preferentially elected as the standby device. This command is available in both the standalone mode and VAC mode. The changed switch ID takes effect only after device restart. In VAC mode, *device_id* indicates the ID of the currently running device. If the device ID does not exist, the configuration does not take effect.

Saving the Configuration File

Run the **exit** command to exit the VAC configuration mode and run the **write** command to save the configuration to the **config_vac.dat** file.

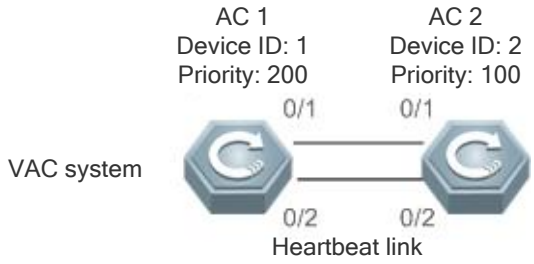
Verification

Run the **show virtual-ac** [**topology | config**] command to display information about the currently running VAC system, topology structure, or VAC system parameters.

Command	**show virtual-ac** [**topology	config**]
Parameter Description	Topology: Indicates the topology information, that is, VAC system configuration information.
Command Mode	Privileged EXEC mode
Usage Guide	Check the domain ID and the device ID, status, and role of each device.

Configuration Example

Configuring VAC System Attributes

Scenario **Figure 4-12**	 AC 1 and AC 2 form a VAC system. Change the device ID of AC 2 to 3 and priority to 150. Assume that AC 1 is the global active device. Complete the configuration on the global active device.
Configuration Steps	● Modify the configuration of AC 2.
AC 2	Ruijie#config Ruijie(config)# virtual-ac domain 100 Ruijie(config-vac-domain)# device 2 renumber 3 Ruijie(config-vac-domain)# device 2 priority 150 Ruijie(config-vac-domain)# device 2 description AC3
Verification	● Run the **show virtual-ac config** command to display the configuration.
AC 1	Ruijie#show virtual-ac config device_id: 1 (mac: 0x1201aeda0M) ! virtual-ac domain 100 ! device 1 device 1 priority 100 ! device convert mode virtual ! port-member interface GigabitEthernet 0/1 ! port-member interface GigabitEthernet 0/2 !
	device_id: 3 (mac: 0x1201aeda0E) ! virtual-ac domain 100

	! device 3 device 3 priority 150 ! device convert mode virtual ! port-member interface GigabitEthernet 1/1 ! port-member interface GigabitEthernet 1/2 ! device 3 description AC3 !

4.4.2.2 Configuring Heartbeat Links

Configuration Effect

- After devices compose a VAC system or when the VAC system is running, if common ports need to be switched to heartbeat ports and vice versa, you can log in to the console of the active device in the VAC system for modification. You cannot enter the global configuration mode from the console of the standby device.

Notes

- You can log in to the console of the VAC system via a serial port or in telnet mode, to add or delete heartbeat ports.

Configuration Steps

Entering the Heartbeat Port Mode

- Run the **vac-port** command to enter the heartbeat port configuration mode. This command is optional.
- When the device enters the heartbeat port configuration mode, you can add or delete heartbeat ports.

Command	**vac-port**
Parameter Description	N/A
Defaults	N/A
Command Mode	Configuration mode
Usage Guide	This command is available in both the standalone mode and VAC mode.

Configuring Heartbeat Ports

- Run the **port-member interface** *interface-name* [**copper** | **fiber**] command to configure a heartbeat port. This command is optional.
- Run the **port-member interface** command to add or delete a heartbeat port.

Command	**port-member interface** *interface-name* [**copper | fiber**]
Parameter Description	*interface-name*: Indicates a 2D port name, for example, GigabitEthernet 0/1 and GigabitEthernet 0/3. **copper**: Indicates the electrical port attribute. **fiber**: Indicates the SFP port attribute.
Defaults	N/A
Command Mode	config-vac-port configuration mode
Usage Guide	This command is available in both VAC mode and standalone mode. In standalone mode, the command configuration needs to be saved and the device where the heartbeat member port resides needs to be restarted for the configuration to take effect. In VAC mode, the command configuration takes effect immediately.

The configured heartbeat member links take effect immediately during the running of the VAC system. Heartbeat ports need to be configured on all devices.

To prevent loops from being instantaneously generated when a heartbeat port is switched to a common port, the system automatically sets the port to be in the shutdown state when this command is executed. You can reconnect the link and run the **no shutdown** command to enable the port.

If the VAC system topology is split because a heartbeat port is switched to a common port, the heartbeat port cannot be deleted. You can disconnect the physical port and then delete the heartbeat port.

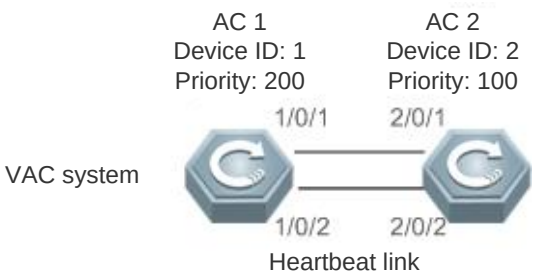
Verification

Run the **show virtual-ac link** [**port**] command to display the running status of the current heartbeat port.

Command	**show virtual-ac link** [**port**]
Parameter Description	**port**: Displays information about a specific port.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring Heartbeat Links

Scenario **Figure 4-13**	
Configuration Steps	● Add Port 1/0/3 as a heartbeat port and remove the heartbeat port 0/2.
	Ruijie#config Ruijie(config)# vac-port Ruijie(config-vac-port)# port-member interface Gigabitethernet 1/0/3 Ruijie(config-vac-port)# no port-member interface Gigabitethernet 1/0/2
Verification	● Run the **show virtual-ac config** command to display heartbeat links. Assume that device-1 is the active device. Run the command on the active device.
	Ruijie#show virtual-ac config device_id: 1 (mac: 0x1201aeda0M) ! Virtual-ac domain 100 ! device 1 device 1 priority 200 ! device convert mode virtual ! port-member interface Gigabitethernet 0/1 ! port-member interface Gigabitethernet 0/3 !
	device_id: 2 (mac: 0x1201aeda0E) ! virtual-ac domain 100 ! device 2 device 2 priority 100 ! device convert mode virtual !

	port-member interface Gigabitethernet 0/1 ! port-member interface Gigabitethernet 0/2 !

4.4.2.3 Configuring Dual-active Detection

Configuration Effect

Configure the relevant detection mechanism to prevent coexistence of dual active devices.

Notes

- Dual-active detection can be configured only in VAC mode.
- Dual-active detection is configured in global configuration mode and the dual-active detection configuration takes effect immediately on the active device. Run the **show running-config** command to display the configuration.
- BFD-based dual-active detection configuration cannot be displayed by running the BFD display command but by running the dual-active detection display command.

Configuration Steps

Configuring BFD-based Dual-active Detection

- In BFD-based dual-active detection, a direct link needs to be established between two chassis and the ports at both ends of the link must be physical routing ports. The following configuration is required on both devices.
- Enter the interface configuration mode of the detection port and configure the detection port as a routing port.
- Exit the interface configuration mode, and run the **virtual-ac domain** *domain_id* command to enter the config-vac-domain configuration mode.
- In config-vac-domain configuration mode, run the **dual-active detection bfd** command to enable the BFD function. This command is optional. Use this command when you need to configure BFD-based dual-active detection.
- In config-vac-domain mode, run the **dual-active bfd interface** *interface-name* command to configure the BFD detection port. This command is optional. When configuring the BFD-based dual-active detection, use this command to configure the BFD detection port.
- If no BFD detection port is available after a BFD detection port is deleted, the BFD detection will be unavailable.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only two devices with the same domain ID can compose a virtual device. The domain ID must be unique in the LAN.

Command	**dual-active detection** { **aggregateport	bfd** }
Parameter Description	**aggregateport**: Specifies the aggregate port-based detection. **bfd**: Indicates BFD detection.
Defaults	The dual-active detection function is disabled.
Command Mode	config-vac-domain configuration mode
Usage Guide	This command can be configured only in VAC mode.

Command	**dual-active bfd interface** *interface-name*
Parameter Description	*interface-name*: Indicates the type and ID of the detection port.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	BFD detection ports must be routing ports and reside in different devices.

- BFD detection ports must be direct physical routing ports and must reside in different devices.
- The configured port type is unlimited. Dual-active detection links are used to transmit only BFD packets, and the traffic is light. Therefore, it is recommended to configure a 1000M or 100M port as the dual-active detection port.
- After a Layer-3 routing port configured for dual-active detection is switched into a Layer-2 switching port (by running the **switchport** command on the port), the BFD dual-active detection configuration is automatically cleared.
- It is recommended to adopt direct connection for the BFD link and the BFD link connects only the active and standby devices.
- When a dual-active conflict is detected and one VAC system is enabled to enter the recovery state, users can rectify the fault by eliminating the VSL failure rather than by directly resetting the VAC system in the recovery state. Otherwise, a dual-active conflict will be incurred in the network.

Configuring Aggregate Port-based Dual-active Detection

- To configure aggregate port-based dual-active detection, configure an aggregate port AP and then specify the aggregate port AP as the detection port.
- Run the **port-group** *ap-num* command to add a physical member port to the aggregate port AP.
- Run the **dual-active interface** *interface-name* command to configure the aggregate port as the dual-active detection port. This command is optional. When configuring aggregate port-based dual-active detection, use this command to configure the aggregate port as the dual-active detection port.

- Run the **dad relay enable** command to enable the function of transferring dual-active detection packets on ports in the upstream and downstream devices. This command is optional. When configuring aggregate port-based dual-active detection, use this command to forward DAD packets (that is, dual-active detection packets).
- Disabling the aggregate port-based dual-active detection will invalidate the dual-active detection of the aggregate port.
- If no detection port is available after a detection port is deleted, the detection will be unavailable.
- The function of forwarding aggregate port-based dual-active detection packets is disabled by default.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only two devices with the same domain ID can compose a virtual device. The domain ID must be unique in the LAN.

Command	**dual-active interface** *interface-name*
Parameter Description	*interface-name*: Indicates the type and ID of the detection port.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	Detection ports must belong to an aggregate port and member ports of the aggregate port must reside in different devices.

It is recommended that physical ports that are added to an aggregate detection port reside in different devices.

When a dual-active conflict is detected and one VAC system is enabled to enter the recovery state, users can rectify the fault by eliminating the heartbeat link failure rather than by directly resetting the VAC system in the recovery state. Otherwise, a dual-active conflict will be incurred in the network.

Configuring Excluded Port List in Recovery Mode

- When dual active devices are detected, one active device must enter the recovery mode. In recovery mode, all service ports of the device need to be disabled. To ensure normal use of service ports for some special purposes (for example, configuring a port for logging in to the management device remotely), users can configure some ports as excluded ports that do not need to be disabled in recovery mode.
- After entering the config-vac-domain configuration mode, run the **dual-active exclude interface** *interface-name* command to specify excluded ports that do not need to be disabled in recovery mode. This command is optional.

Command	**dual-active exclude interface** *interface-name*

Parameter Description	*interface-name*: Indicates the type and ID of a port.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command can be configured only in VAC mode. Excluded ports must be routing ports and cannot be heartbeat ports. You can configure multiple excluded ports.

Excluded ports must be routing ports and cannot be heartbeat ports.

After a routing port is switched into a switching port (run the **switchport** command on the port), the excluded port configuration associated with the routing port is automatically cleared.

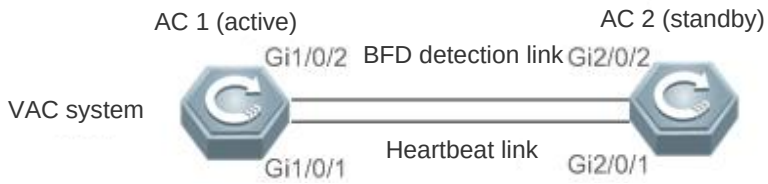
Verification

Run the **show virtual-ac dual-active summary** command to display the current dual-active configuration.

Command	**show virtual-ac dual-active summary**
Parameter Description	**smmary**: Displays the DAD summary.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring BFD-based Dual-active Detection

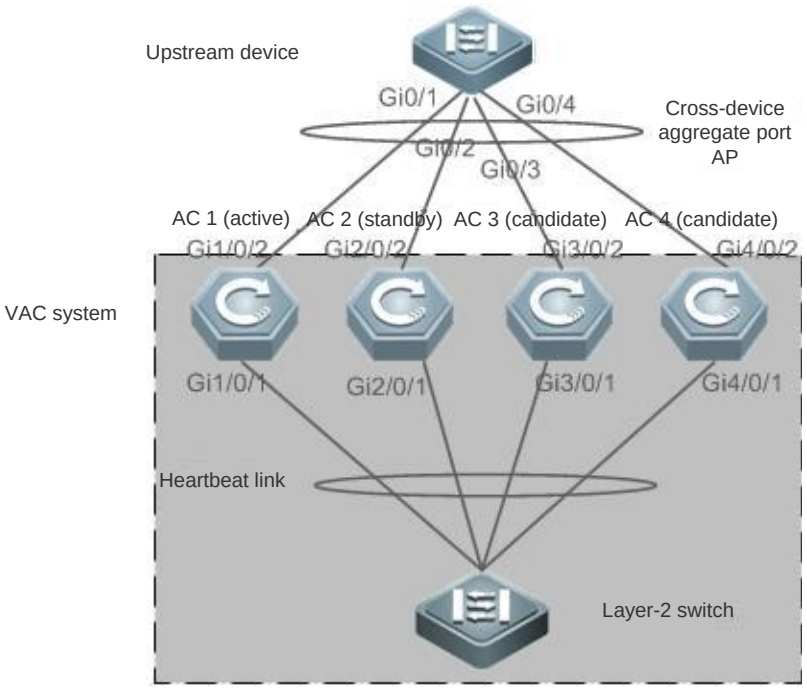
Scenario Figure 4-14	 ● Device 1 and Device 2 compose a VAC system (the domain ID is 100). The priority of Device 1 is 200 and the priority of Device 2 is 150. A connection is established between Port Gi1/0/1 of Device 1 and Port Gi2/0/1 of Device 2, which forms the VSL between Device 1 and Device 2. Port Gi1/0/2 of Device 1 is connected to Port G2/0/2 of Device 2. Ports G1/0/2 and G2/0/2 are both routing ports. ● Ports G1/0/2 and G2/0/2 are a pair of BFD dual-active detection ports.
Configuration Steps	● Configure Port G1/0/2 and Port G2/0/2 as routing ports. ● Enable the BFD-based dual-active detection. ● Configure Port G1/0/2 and Port G2/0/2 as BFD detection ports. Device 1 and Device 2 form a VAC system. Therefore, the configuration above can be performed on either Device 1 or Device 2. Here uses Device 1 as an example.

Switch 1	Ruijie(config)# interface GigabitEthernet 1/0/2 Ruijie(config-if-GigabitEthernet 1/0/2)# no switchport Ruijie(config)# interface GigabitEthernet 2/0/2 Ruijie(config-if-GigabitEthernet 2/0/2)# no switchport Ruijie(config-if)# virtual-ac domain 100 Ruijie(config-vac-domain)# dual-active detection bfd Ruijie(config-vac-domain)# dual-active bfd interface GigabitEthernet 1/0/2 Ruijie(config-vac-domain)# dual-active bfd interface GigabitEthernet 2/0/2
Verification	● Check the status of the dual-active detection function. ● Check the BFD-based dual-active detection configuration.
Switch 1	Ruijie# show switch virtual dual-active summary BFD dual-active detection enabled: Yes Aggregateport dual-active detection enabled: No Interfaces excluded from shutdown in recovery mode: In dual-active recovery mode: NO Ruijie# show switch virtual dual-active bfd BFD dual-active detection enabled: Yes BFD dual-active interface configured: GigabitEthernet 1/0/2: UP GigabitEthernet 2/0/2: UP

Common Errors

- A BFD detection port is not a routing port.
- Both BFD-based dual-active detection and aggregate port-based dual-active detection are activated.

Configuring Aggregate Port-based Dual-active Detection

Scenario **Figure 4-15**	 ● AC 1, AC 2, AC 3, and AC 4 form a VAC system (the domain ID is 1). The priority of AC 1 is 200, and the priorities of AC 2, AC 3, and AC4 are all 150. Ports Gi1/0/1, Gi2/0/1, Gi3/0/1, and Gi4/0/1 of the VAC system establish connections to the Layer-2 switch, which form the heartbeat links of the VAC system. Ports G0/1, G0/2, G0/3, and G0/4 of the upstream device are respectively connected to Ports G1/0/2, G2/0/2, G3/0/2, and G4/0/2 of the VAC system to form an aggregate port group that covers four member links. The ID of the aggregate port group is 1. All members of Aggregate Port Group 1 are GE SFP ports.
Configuration Steps	● Configure Aggregate Port Group 1 as the dual-active detection port.
AC 1	`Ruijie(config)# virtual-ac domain 100` `Ruijie(c config-vs-domain)# dual-active detection aggregateport` `Ruijie(config-vac-domain)# dual-active interface aggregateport 1`
Layer-2 Switch	`Ruijie# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#interface  aggregateport 1` `Ruijie(config-if-AggregatePort 1)#dad relay enable`
Verification	● Check the status of the dual-active detection function.
AC 1	`Ruijie#show virtual-ac dual-active summary` `BFD dual-active detection enabled: No` `Aggregateport dual-active detection enabled: Yes` `Interfaces excluded from shutdown in recovery mode:` `In dual-active recovery mode: No`

	Ruijie#show virtual-ac dual-active aggregateport Aggregateport dual-active detection enabled: Yes Aggregateport dual-active interface configured: AggregatePort 1: UP GigabitEthernet 1/0/2: UP GigabitEthernet 2/0/2: UP GigabitEthernet 3/0/2: UP GigabitEthernet 4/0/2: UP

Common Errors

- A dual-active detection port is not an aggregate port.

4.4.2.4 Configuring Standby Device Preemption

Configuration Effect

Configure standby device preemption to reduce the cases that the active and standby devices are faulty simultaneously.

Notes

- The standby device preemption can be configured only in VAC mode.
- Standby device preemption is configured in global configuration mode and the configuration takes effect immediately on the active device. Run the **show running-config** command to display the configuration.

Configuration Steps

Configuring Standby Device Preemption

Configuration Steps	• Configure standby device preemption.
AC 1	Ruijie(config)# virtual-ac domain 100 Ruijie(config-vs-domain)# slave preemptive enable
Verification	• Check the status of the dual-active detection function.
AC 1	Ruijie#show running-config virtual-ac domain 100 slave preemptive enable

4.5 Monitoring

Displaying

Description	Command

Displays information about the currently running VAC system, topology structure, or current VAC system parameters.	**show virtual-ac** [**topology | config | role**]
Displays the current dual-active detection configuration.	**show virtual-ac dual-active summary**
Displays the heartbeat link running status in VAC mode.	**show virtual-ac link** [**port**]
Redirects to the console of the active device or any device.	**session** { **device** *device_id* | **master** }
Displays the device ID.	**show device id**

5 Configuring Bonjour Gateway

5.1 Overview

The Bonjour gateway is used to manage the clients and servers supporting the Bonjour protocol, to implement Bonjour applications in large-scale networks.

The Bonjour gateway provides the following functions:

- Controls the traffic of mDNS packets in the network to decrease excessive mDNS packets.
- Configures Bonjour policies and rules to manage the available services on the client.
- Forwards the mDNS packets of clients and servers across VLANs to enhance ease of use for networks.

Protocols and Standards

- RFC 1034: Domain Names - Concepts and Facilities
- RFC 1035: Domain Names - Implementation and Specification
- RFC 6762: Multicast DNS

5.2 Applications

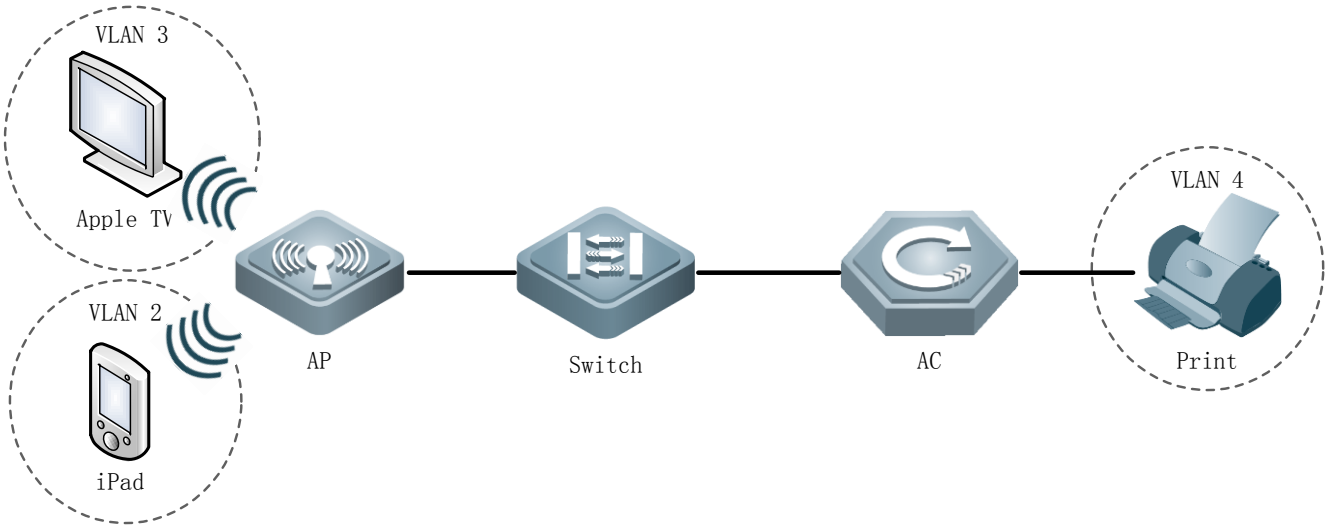
Application	Description
Query Proxy and Response Forwarding	In some cases, the Bonjour gateway receives query packets from a client, but its service resource entries show that it does not obtain the specified service requested by the client. In this case, the Bonjour gateway needs to perform query proxy and response forwarding on the specified service. When the Bonjour gateway forwards the query packets and receives response packets about the service, it adds information about the service to the Bonjour service resource entries, and forwards the response packets to the client. Then, the Bonjour gateway can perform response proxy for the server.

5.2.1 Query Proxy and Response Forwarding

Scenario

As shown in the following figure, iPad, Apple TV, and Print are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and Print through the Bonjour gateway to communicate with them.

Figure 5-1 Bonjour Gateway Topology



Deployment

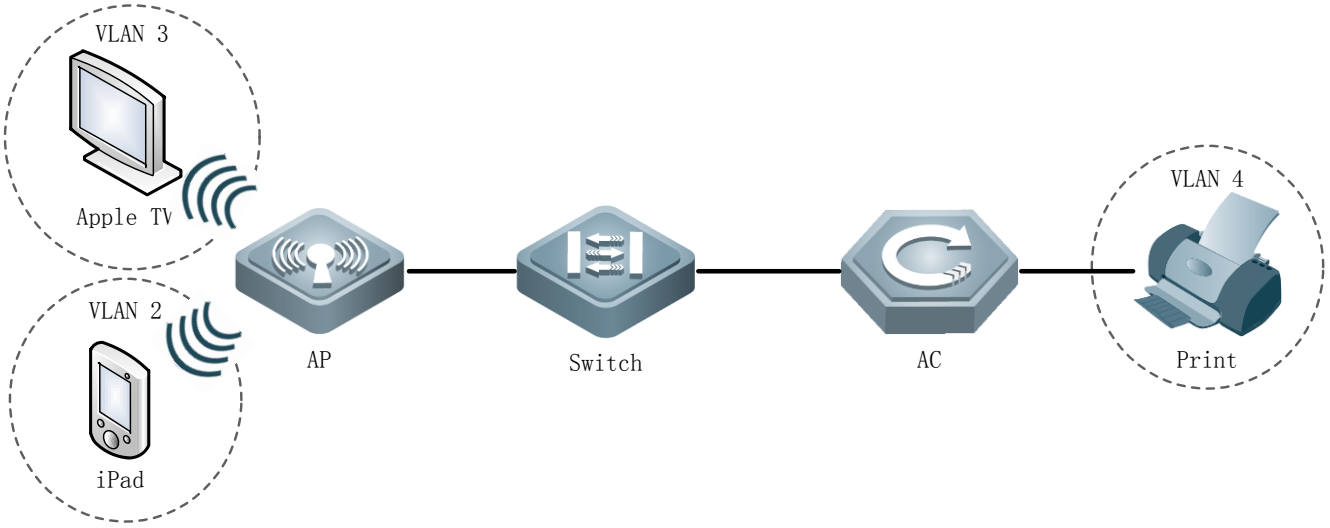
- Enable the Bonjour gateway globally to process the multicast DNS request packets received on the interface.

5.2.2 Preemption Prohibition of the Multimedia Gateway

Scenario

As shown in the following figure, iPad, Apple TV, and Print are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and Print through the Bonjour gateway to communicate with them. When different clients use the screen projection function of Apple TV at the same time, they may preempt the function if the Bonjour gateway is not enabled. When the Bonjour gateway is enabled, preemption prohibition can be implemented.

Figure 5-2 Bonjour Gateway Topology



Deployment

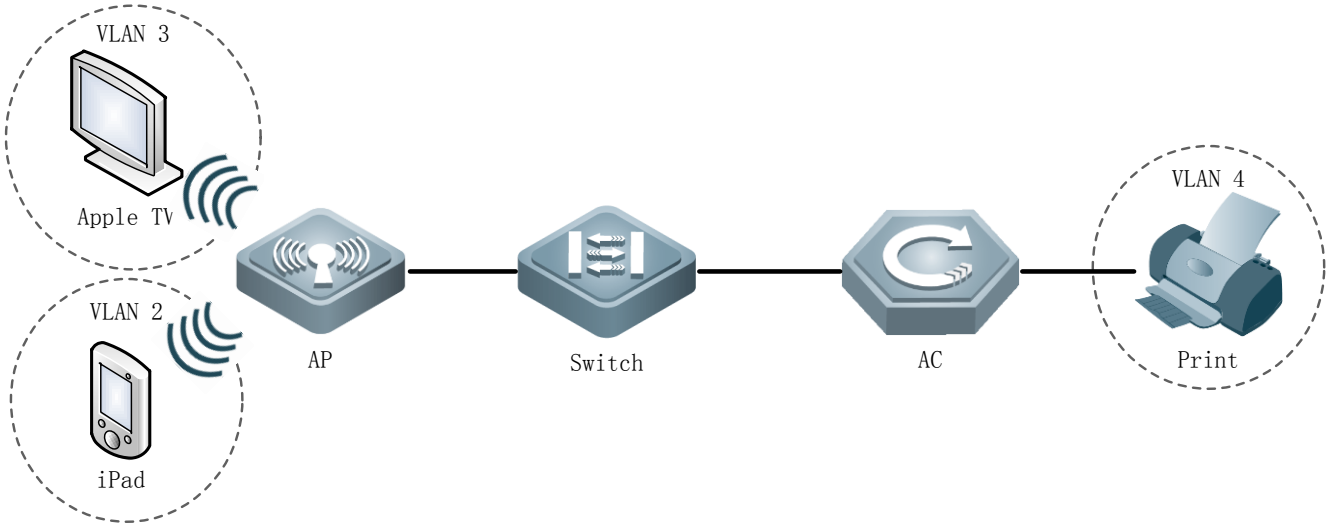
- Enable the Bonjour gateway globally to process the multicast DNS request packets received on the interface and enable preemption prohibition. Preemption prohibition is forcedly enabled, and cannot be disabled.

5.2.3 Automatic Server Renaming of the Multimedia Gateway

Scenario

As shown in the following figure, iPad, Apple TV, and Print are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and Print through the Bonjour gateway to communicate with them. If multiple Apple TVs exist in the network, the same name may be displayed for the projectors on the clients. This function enables automatic server renaming in the form of name + IP address to differentiate them.

Figure 5-3 Bonjour Gateway Topology



Deployment

- Enable the Bonjour gateway globally to process the multicast DNS request packets received on the interface and automatically rename the discovered servers.

5.3 Features

Basic Concepts

Bonjour

Bonjour is the name of the multicast DNS–based open zero-configuration network standard given by Apple. Devices using Bonjour automatically transmit their own service information in the network and listen to service information of other devices, just like saying hello to each other. In this way, Bonjour makes the systems and services in a LAN easily found even if there

is no network administrator. Bonjour displays the names of devices and applications supporting the multicast domain name protocol in a LAN, and uses the multicast DNS to eliminate device naming conflicts.

Bonjour Gateway

The Bonjour gateway is used to manage the clients and servers supporting the Bonjour protocol, to implement Bonjour applications in large-scale networks.

Overview

Feature	Description
Bonjour Gateway	The Bonjour gateway is used to manage the clients and servers supporting the Bonjour protocol, to implement Bonjour applications in large-scale networks.

5.3.1 Bonjour Gateway

Working Principle

The Bonjour gateway is used to manage the clients and servers supporting the Bonjour protocol, to implement Bonjour applications in large-scale networks.

The Bonjour gateway provides the following functions:

Response Proxy

Servers send Bonjour response packets in the network to advertise the services they support. After receiving the response packets, the Bonjour gateway establishes Bonjour service resource entries, and directly sends response packets to the clients that query services contained in the entries.

Query Proxy and Response Forwarding

In some cases, the Bonjour gateway receives query packets from a client, but its service resource entries show that it does not obtain the specified service requested by the client. In this case, the Bonjour gateway needs to perform query proxy and response forwarding on the specified service. When the Bonjour gateway forwards the query packets and receives response packets about the service, it adds information about the service to the Bonjour service resource entries, and forwards the response packets to the client. Then, the Bonjour gateway can perform response proxy for the server.

Screen Preemption Prohibition

When different clients use the screen projection function of Apple TV at the same time, they may preempt the function if the Bonjour gateway is not enabled. When the Bonjour gateway is enabled, preemption prohibition can be implemented.

Automatic Renaming of Servers

If multiple Apple TVs exist in the network, the same name may be displayed for the projectors on the clients. This function enables automatic server renaming in the form of name + IP address to differentiate them.

5.4 Configuration

Configuration	Description and Command	
Enabling the Bonjour Gateway	⚠ Mandatory. It is used to create the Bonjour gateway service.	
	bonjour-gateway enable	Enables the Bonjour gateway.
	⚠ Optional.	
Configuring Bonjour Policies and Rules	⚠ Optional.	
	bonjour-gateway global-strategy	Applies a specified Bonjour policy globally.
	bonjour-gateway strategy	Applies a specified Bonjour policy on interfaces.
	bonjour-gateway strategy-mode	Creates a Bonjour policy.
	service type	Configures a service rule.
	service vlan range	Configures a VLAN that allows forwarding query and response packets.
	service wired/wireless	Enables service discovery in wired or wireless mode.
Configuring Preemption Prohibition and Automatic Renaming	**bonjour-gateway airplay-preemption disable**	Disables preemption prohibition.
	bonjour-gateway airplay-rename disable	Disables automatic renaming.
Actively Querying Bonjour Services	⚠ Optional.	
	bonjour-gateway query enable	Enables the active query of Bonjour services.
	bonjour-gateway query interval	Configures the interval for actively querying Bonjour services.

5.4.1 Enabling the Bonjour Gateway

Configuration Effect

- Implement Bonjour applications in large-scale networks after enabling the Bonjour gateway.

Notes

- The Bonjour gateway must be enabled on Layer-3 interfaces.

Configuration Steps

↘ **Enabling the Bonjour Gateway**

- Mandatory.

Command	**bonjour-gateway enable**
Parameter Description	N/A
Defaults	The Bonjour gateway is disabled by default.
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	After this function is configured, multicast is enabled on all or specified Layer-3 interfaces to forward multicast packets. The global Bonjour gateway must be enabled before enabling Bonjour gateway on a specified interface.

Configuring the Threshold of Multicasting Response Packets

- Optional.
- Run the **bonjour-gateway multicast** command to configure the threshold of multicasting response packets.

Command	**bonjour-gateway multicast** *number*
Parameter Description	*number*: Sets the threshold of multicasting response packets. The value ranges from **1** to **64**.
Defaults	The threshold of multicasting response packets is **10** by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway multicast** command is used to configure the threshold of multicasting response packets. The **no bonjour-gateway multicast** command is used to restore the default settings. By default, the threshold of multicasting response packets is **10**.

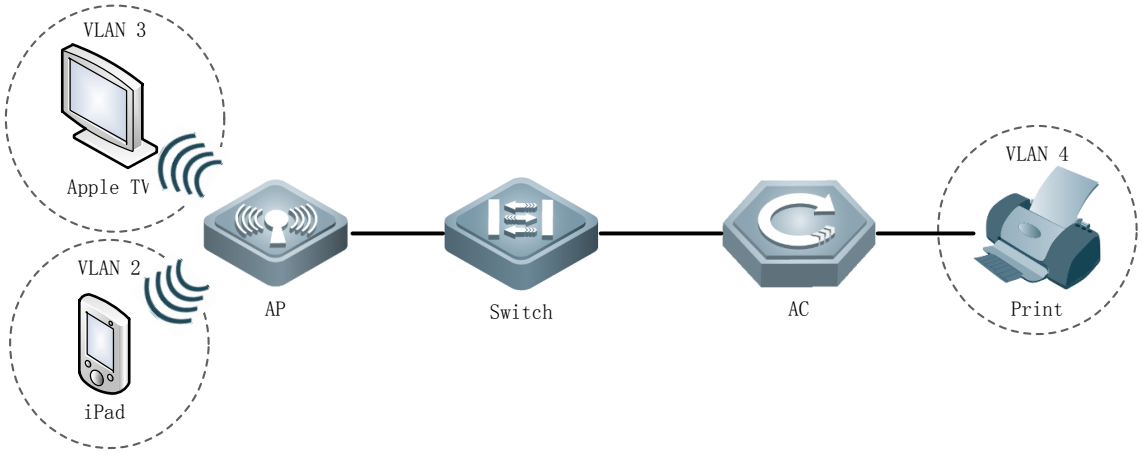
Verification

- Run the **show run** command to display the Bonjour gateway configurations.

Configuration Example

Enabling the Bonjour Gateway

Scenario Figure 5-4	iPad, Apple TV, and Print are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and Print through the Bonjour gateway to communicate with them.

	
Configuration Steps	● Enable the Bonjour gateway.
	`Ruijie#configure terminal` `Ruijie(config)#` `Ruijie(config)#interface vlan 2` `Ruijie(config-if-vlan 2 )#bonjour-gateway enable`
Verification	● Check whether the Bonjour gateway is enabled. `Ruijie#show run | begin interface vlan 2` `Current configuration : 491 bytes` `interface vlan 2` ` bonjour-gateway enable` `!`

5.4.2 Configuring Bonjour Policies and Rules

Configuration Effect

- Configure Bonjour policies and rules to manage the available services on the client.

Configuration Steps

↘ Creating a Bonjour Policy

- Optional.
- Run the **bonjour-gateway strategy-mode** command to create a Bonjour policy.

Command	**bonjour-gateway strategy-mode** *name*
Parameter Description	*name*: Indicates the name of a Bonjour policy.
Defaults	No Bonjour policy is created by default.

Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway strategy-mode** command is used to create a Bonjour policy. The **no bonjour-gateway strategy-mode** command is used to delete a Bonjour policy. By default, no Bonjour policy is created. A maximum of 1000 Bonjour policies can be created on the device.

Configuring a Service Discovery Rule

- Optional.
- Run the **service [wired | wireless] disable** command to configure a service discovery rule.

Command	**service [wired | wireless] disable**
Parameter Description	N/A
Defaults	Services can be discovered in both wired and wireless modes by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service [wired | wireless] disable** command is used to configure a service discovery rule. The **no service [wired | wireless] disable** command is used to delete a service discovery rule. By default, service discovery is allowed in both wired and wireless modes.

Configuring a Service Instance

- Optional.
- Run the **service type** command to set a service rule.

Command	**service type** *type* **[instance** *name* | **disable]**
Parameter Description	*type*: Indicates the type of a service that can be found by the client. *name*: Indicate the instance name of a service that needs to be searched for by the client.
Defaults	The client can find all services by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service type** command is used to set a service rule. The **no service type** command is used to delete a service rule. By default, the client can find all services. After the **no service type** command is configured, the corresponding service cannot be found.

Configuring a Service VLAN

- Optional.
- Run the **service vlan range** command to configure a VLAN that allows forwarding query and response packets when a specified Bonjour policy is applied.

Command	**service vlan** range *vlan-id-list* **[access-vlan]**
Parameter Description	*vlan-id-list*: Indicates the VLAN list. **access-vlan**: Allows forwarding query and response packets in the client-accessed VLAN.

Defaults	All query and response packets are forwarded by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service vlan range** command is used to configure a VLAN that allows forwarding query and response packets, and discard the query and response packets outside the VLAN. The **no service vlan** command is used to delete the settings. By default, all query and response packets are forwarded.

Applying a Specified Bonjour Policy Globally

- Optional.
- Run the **bonjour-gateway global-strategy** command to apply a specified Bonjour policy globally.

Command	**bonjour-gateway global-strategy** *name*
Parameter Description	*name*: Indicates the name of a Bonjour policy.
Defaults	No Bonjour policy is applied globally by default.
Command Mode	Configuration mode
Usage Guide	The **bonjour-gateway global-strategy** command is used to apply a specified Bonjour policy globally. The **no bonjour-gateway global-strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied globally. That is, when the Bonjour gateway is enabled, only the default service type is supported by default, and services can be found in both wired and wireless modes.

Applying a Specified Bonjour Policy

- Optional.
- Run the **bonjour-gateway strategy** command to apply a specified Bonjour policy on Layer-3 interfaces.

Command	**bonjour-gateway strategy** *name*
Parameter Description	*name*: Indicates the name of a Bonjour policy.
Defaults	No Bonjour policy is applied on Layer-3 interfaces by default.
Command Mode	Interface configuration mode
Usage Guide	The **bonjour-gateway strategy** command is used to apply a specified Bonjour policy on Layer-3 interfaces. The **no bonjour-gateway strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied on Layer-3 interfaces.

Verification

- Run the **show run** command to display the Bonjour gateway configurations.

Configuration Example

Configuring a Bonjour Policy

Scenario	For details, refer to Figure 5-4.
Configuration Steps	Configure a Bonjour policy.
	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# bonjour-gateway strategy-mode teacher Ruijie(config-bonjour-gateway)#service type ftp ip 10.0.0.5 Ruijie(config-bonjour-gateway)#service vlan range 5 Ruijie(config-bonjour-gateway)#service vlan access-vlan Ruijie(config-bonjour-gateway)#exit Ruijie(config)# Ruijie(config)#interface vlan 2 Ruijie(config-if-vlan 1)#bonjour-gateway enable Ruijie(config-if-vlan 1)# bonjour-gateway strategy teacher
Verification	● Check whether the Bonjour gateway is enabled. Ruijie#show run | begin interface VLAN 1 Current configuration : 491 bytes interface VLAN 2 bonjour-gateway enable bonjour-gateway strategy teacher ! ● Check whether a Bonjour policy is configured. Ruijie#show run | begin bonjour-gateway Current configuration : 491 bytes bonjour-gateway strategy-mode teacher service type ftp ip 10.0.0.5 service vlan range 5 service vlan access-vlan !

5.4.3 Configuring Preemption Prohibition and Automatic Renaming

Configuration Effect

- Configure preemption prohibition and automatic renaming.

Configuration Steps

Disabling Preemption Prohibition

- Optional.
- Run the **bonjour-gateway airplay-preemption disable** command to disable preemption prohibition.

Command	bonjour-gateway airplay-preemption disable
Parameter Description	N/A
Defaults	Preemption prohibition is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway airplay-preemption disable** command is used to disable preemption prohibition.

Disabling Automatic Renaming

- Optional.
- Run the **bonjour-gateway airplay-rename disable** command to disable automatic renaming.

Command	bonjour-gateway airplay-rename disable
Parameter Description	N/A
Defaults	Automatic renaming is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway airplay-rename disable** command is used to disable automatic renaming.

Verification

- Run the **show run** command to display the Bonjour gateway configurations.

Configuration Example

Disabling Automatic Renaming

Scenario	For details, refer to Figure 5-4.
Configuration Steps	Disable automatic renaming.
	`Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)# bonjour-gateway airplay-rename disable`

Verification	● Check whether automatic renaming is disabled. `Ruijie#show run | begin bonjour-gateway` `Current configuration : 491 bytes` `bonjour-gateway airplay-rename disable!`

Common Errors

5.4.4 Active Query of Bonjour Services

Configuration Effect

- To implement response proxy, the Bonjour gateway needs to maintain the Bonjour service resource entries. When the active query of Bonjour services is enabled, the Bonjour gateway can guarantee the real-timeliness of Bonjour service resource entries.

Configuration Steps

↘ Enabling the Active Query of Bonjour Services

- Optional.
- Run the **bonjour-gateway query enable** command to enable the active query of Bonjour services.

Command	**bonjour-gateway query enable**
Parameter Description	N/A
Defaults	The active query of Bonjour services is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway query enable** command is used to enable the active query of Bonjour services. The **no bonjour-gateway query enable** command is used to disable the active query of Bonjour services. By default, the active query of Bonjour services is disabled.

↘ Configuring the Interval for Sending Query Packets to a Discovered Service

- Optional.
- Run the **bonjour-gateway query interval** command to configure the interval for sending query packets to a discovered service.

Command	**bonjour-gateway query interval** *number*
Parameter Description	*number*: Indicates the interval for sending query packets to a discovered service in seconds. The value ranges from **5** to **600**.
Defaults	The interval for sending query packets to a discovered service is 15 seconds by default.
Command Mode	Global configuration mode

Usage Guide	The **bonjour-gateway query interval** command is used to configure the interval for sending query packets to a discovered service. The **no bonjour-gateway query interval** command is used to restore the default settings. By default, the interval for sending query packets to a discovered service is 15 seconds.

Verification

- Run the **show run** command to display the Bonjour gateway configurations.

Configuration Example

Enabling the Active Query of Bonjour Services

Scenario	For details, refer to Figure 5-4.
Configuration Steps	Enable the active query of Bonjour services.
	`Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#bonjour-gateway query enable` `Ruijie(config)#bonjour-gateway query interval 20`
Verification	● Check whether the active query of Bonjour services is enabled. `Ruijie#show run | begin bonjour-gateway` `Current configuration : 491 bytes` `bonjour-gateway query enable` `bonjour-gateway query interval 20` `!`

5.5 Monitoring

Displaying

Description	Command
Displays information about the discovered Bonjour service.	**show bonjour-gateway service-database**
Displays information about the discovered Bonjour service of a specified IP.	**show bonjour-gateway service-database ip** *address*
Displays the Bonjour policy information.	**show bonjour-gateway strategy-mode**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the Bonjour gateway error.	**debug bonjour error**
Debugs preemption of the Bonjour gateway.	**debug bonjour stamng**

Access Service Configuration

1. Configuring Interfaces
2. Configuring MAC Address
3. Configuring Aggregated Port
4. Configuring VLAN
5. Configuring Super VLAN
6. Configuring MSTP
7. Configuring VLAN Group
8. Configuring PPPoE-Client
9. Configuring RLDP
10. Configuring LLDP
11. Configuring DLDP

1 Configuring Interfaces

1.1 Overview

Interfaces are important in implementing data switching on network devices. Ruijie devices support two types of interfaces: physical ports and logical interfaces. A physical port is a hardware port on a device, such as the 100M Ethernet interface and gigabit Ethernet interface. A logical interface is not a hardware port on the device. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical port or independent of any physical port. For network protocols, physical ports and logical interfaces serve the same function.

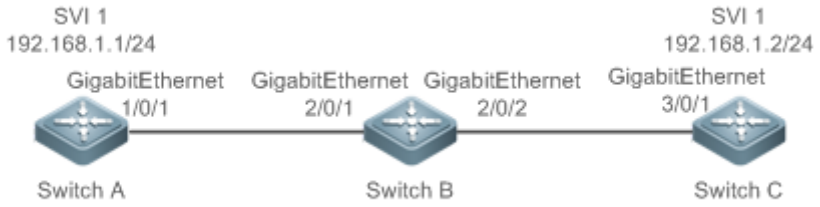
1.2 Applications

Application	Description
L2 Data Switching Through the Physical Ethernet Interface	Implement Layer-2 (L2) data communication of network devices through the physical L2 Ethernet interface.
L3 Routing Through the Physical Ethernet Interface	Implement Layer-3 (L3) data communication of network devices through the physical L3 Ethernet interface.

1.2.1 L2 Data Switching Through the Physical Ethernet Interface

Scenario

Figure 1-1



As shown in Figure 1-1 , Switch A, Switch B, and Switch C form a simple L2 data switching network.

Deployment

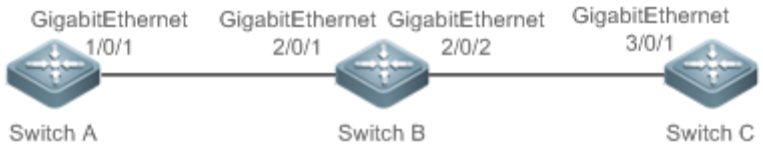
- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as Trunk ports.

- Create a switch virtual interface (SVI), SVI 1, on Switch A and Switch C respectively, and configure IP addresses from a network segment for the two SVIs. The IP address of SVI 1 on Switch A is 192.168.1.1/24, and the IP address of SVI 1 on Switch C is 192.168.1.2/24.
- Run the **ping 192.168.1.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement data switching through Switch B.

1.2.2 L3 Routing Through the Physical Ethernet Interface

Scenario

Figure 1-2



As shown in Figure 1-2, Switch A, Switch B, and Switch C form a simple L3 data communication network.

Deployment

- Connect Switch A to Switch B through physical ports GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through physical ports GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1.
- Configure GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2, and GigabitEthernet3/0/1 as L3 routed ports.
- Configure IP addresses from a network segment for GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1. The IP address of GigabitEthernet 1/0/1 is 192.168.1.1/24, and the IP address of GigabitEthernet 2/0/1 is 192.168.1.2/24.
- Configure IP addresses from a network segment for GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1. The IP address of GigabitEthernet 2/0/2 is 192.168.2.1/24, and the IP address of GigabitEthernet 3/0/1 is 192.168.2.2/24.
- Configure a static route entry on Switch C so that Switch C can directly access the network segment 192.168.1.0/24.
- Run the **ping 192.168.2.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement L3 routing through Switch B.

1.3 Features

Basic Concepts

↘ Interface Classification

Interfaces on Ruijie devices fall into three categories:

- L2 interfaceL3 interface (supported by L3 devices)

1. Common L2 interfaces are classified into the following types:

- Switch port
- L2 aggregate port (AP)

2. Common L3 interfaces are classified into the following types:

- Routed port
- L3 AP port
- SVI
- Loopback interface
- Tunnel interface

Switch Port

A switch port is an individual physical port on the device, and implements only the L2 switching function. The switch port is used to manage physical ports and L2 protocols related to physical ports.

L2 AP Port

An AP port is formed by aggregating multiple physical ports. Multiple physical links can be bound together to form a simple logical link. This logical link is called an AP port.

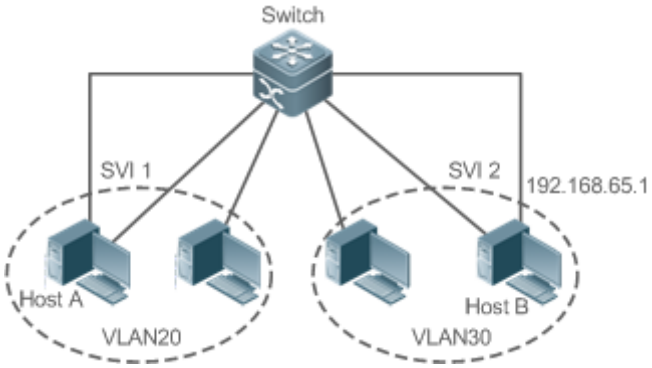
For L2 switching, an AP port is equivalent to a switch port that combines bandwidths of multiple ports, thus expanding the link bandwidth. Frames sent over the L2 AP port are balanced among the L2 AP member ports. If one member link fails, the L2 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

SVI

The SVI can be used as the management interface of the local device, through which the administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each VLAN to implement routing across VLANs among L3 devices. You can run the **interface vlan** command to create an SVI and assign an IP address to this interface to set up a route between VLANs.

As shown in Figure 1-3, hosts in VLAN 20 can directly communicate with each other without participation of L3 devices. If Host A in VLAN 20 wants to communicate with Host B in VLAN 30, SVI 1 of VLAN 20 and SVI 2 of VLAN 30 must be used.

Figure 1-3



Routed Port

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. A routed port is not related with a specific VLAN. Instead, it is just an access port. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

If a port is a L2 AP member port or a DOT1X port that is not authenticated, you cannot run the **switchport** or **no switchport** command to configure the switch port or routed port.

L3 AP Port

Like the L2 AP port, a L3 AP port is a logical port that aggregates multiple physical member ports. The aggregated ports must be the L3 ports of the same type. The AP port functions as a gateway interface for L3 switching. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP port are balanced among the L3 AP member ports. If one member link fails, the L3 AP port automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.

A L3 AP port cannot be used for L2 switching. You can run the **no switchport** command to change a L2 AP port that does not contain any member port into a L3 AP port, add multiple routed ports to this L3 AP port, and then assign an IP address to this L3 AP port to set up a route.

Loopback Interface

The loopback interface is a local L3 logical interface simulated by the software that is always UP. Packets sent to the loopback interface are processed on the device locally, including the route information. The IP address of the loopback interface can be used as the device ID of the Open Shortest Path First (OSPF) routing protocol, or as the source address used by Border Gateway Protocol (BGP) to set up a TCP connection. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface, and you can treat the loopback interface as a virtual Ethernet interface.

Tunnel Interface

The Tunnel interface implements the tunnel function. Over the Tunnel interface, transmission protocols (e.g., IP) can be used to transmit packets of any protocol. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. Instead of specifying any transmission protocol or load protocol, the tunnel interface provides a standard point-to-point (P2P) transmission mode. Therefore, a tunnel interface must be configured for every individual link.

Overview

Feature	Description
Interface Configuration Commands	You can configure interface-related attributes in interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created.
Interface Description and Administrative Status	You can configure a name for an interface to identify the interface and help you remember the functions of the interface. You can also configure the administrative status of the interface.
MTU	You can configure the maximum transmission unit (MTU) of a port to limit the length of a frame that can be received or sent over this port.
Bandwidth	You can configure the bandwidth of an interface.

Feature	Description
Load Interval	You can specify the interval for load calculation of an interface.
Carrier Delay	You can configure the carrier delay of an interface to adjust the delay after which the status of an interface changes from Down to Up or from Up to Down.
Link Trap Policy	You can enable or disable the link trap function on an interface.
Interface Index Persistence	You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.
Routed Port	You can configure a physical port on a L3 device as a routed port, which functions as the gateway interface for L3 switching.
L3 AP Port	You can configure an AP port on a L3 device as a L3 AP port, which functions as the gateway interface for L3 switching.
Selection of Interface Medium Type	You can select the medium type (fiber or copper) of a combo port as required.
Interface Speed, Duplex Mode	You can configure the speed, duplex mode, flow control mode, and auto negotiation mode of an interface.
Automatic Module Detection	If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.
Port Errdisable Recovery	After a port is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recover all the ports in errdisable state and enable these ports.

1.3.1 Interface Configuration Commands

üRun the interface command in global configuration mode to enter interface configuration mode. You can configure interface-related attributes in interface configuration mode.

Working Principle

Run the interface command in global configuration mode to enter interface configuration mode. If you enter interface configuration mode of a non-existing logical interface, the interface will be created. You can also run the interface range or interface range macro command in global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same features.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

↘ Interface Numbering Rules

In stand-alone mode, the ID of a physical port consists of two parts: slot ID and port ID on the slot. For example, if the slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 2/3. In VSU or stack mode, the ID of a physical port consists of three parts: device ID, slot ID, and port ID on the slot. For example, if the device ID is 1, slot ID of the port is 2, and port ID on the slot is 3, the interface ID is 1/2/3.

The device ID ranges from 1 to the maximum number of supported member devices.

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Assume that you are facing the device panel. Dynamic slot are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of a port on the slot ranges from 1 to the number of ports on the slot, and is numbered sequentially from left to right.

You can select fiber or copper as the medium of a combo port. Regardless of the medium selected, the combo port uses the same port ID.

The ID of an AP port ranges from 1 to the number of AP ports supported by the device.

The ID of an SVI is the VID of the VLAN corresponding to this SVI.

Configuring Interfaces Within a Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at a time. Attributes configured in interface configuration mode apply to all these interfaces.

The **interface range** command can be used to specify several interface ranges.

The **macro** parameter is used to configure the macro corresponding to a range. For details, see "Configuring Macros of Interface Ranges."

Ranges can be separated by commas (,).

The types of interfaces within all ranges specified in a command must be the same.

Pay attention to the format of the **range** parameter when you run the **interface range** command.

The following interface range formats are valid:

- **FastEtherne**t device/slot/{first port} - {last port};
- **GigabitEthernet** device/slot/{first port} - {last port};
- **TenGigabitEthernet** device/slot/{first port} - {last port};
- **FortyGigabitEthernet** device/slot/{first port} - {last port};
- **AggregatePort** *Aggregate-port ID* (The AP ID ranges from 1 to the maximum number of AP ports supported by the device.)
- **vlan** vlan-ID-vlan-ID (The VLAN ID ranges from 1 to 4,094.)
- **Loopback** loopback-ID (The loopback ID ranges from 1 to 2,147,483,647.)
- **Tunnel** tunnel-ID (The tunnel ID ranges from 0 to the maximum number of tunnel interfaces supported by the device minus 1.)

Interfaces in an interface range must be of the same type, namely, FastEthernet, GigabitEthernet, AggregatePort, or SVI.

Configuring Macros of Interface Ranges

You can define some macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, you must first run the **define interface-range** command in global configuration mode to define these macros.

Run the **no define interface-range macro_name** command in global configuration mode to delete the configured macros.

1.3.2 Interface Description and Administrative Status

You can configure a name for an interface to identify the interface and help you remember the functions of the interface.

You can enter interface configuration mode to enable or disable an interface.

Working Principle

Interface Description

You can configure the name of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 1/1 for exclusive use by user A, you can describe the interface as "Port for User A."

Interface Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface, and the interface will loss all its functions. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

1.3.3 MTU

You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.

Working Principle

When a large amount of data is exchanged over a port, frames greater than the standard Ethernet frame may exist. This type of frame is called jumbo frame. The MTU is the length of the valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If a port receives or sends a frame with a length greater than the MTU, this frame will be discarded.

The range of MTU is from 64 to 9216 characters. By default, it is 1500 characters.

The command takes effect only on physical port and AP port.

1.3.4 Bandwidth

Working Principle

The **bandwidth** command can be configured so that some routing protocols (for example, OSPF) can calculate the route metric and the Resource Reservation Protocol (RSVP) can calculate the reserved bandwidth. Modifying the interface bandwidth will not affect the data transmission rate of the physical port.

The **bandwidth** command is a routing parameter, and does not affect the bandwidth of a physical link.

1.3.5 Load Interval

Working Principle

You can run the **load-interval** command to specify the interval for load calculation of an interface. Generally, the interval is 10s.

1.3.6 Carrier Delay

Working Principle

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from Down to Up or from Up to Down. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If this parameter is set to a great value, nearly every DCD change is not detected. On the contrary, if the parameter is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, the carrier delay should be set to a smaller value to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, the carrier delay should be set to a greater value to avoid topology or route flapping.

1.3.7 Link Trap Policy

You can enable or disable the link trap function on an interface.

Working Principle

When the link trap function on an interface is enabled, the Simple Network Management Protocol (SNMP) sends link traps when the link status changes on the interface.

1.3.8 Interface Index Persistence

Like the interface name, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

Working Principle

After interface index persistence is enabled, the interface index remains unchanged after the device is restarted.

1.3.9 Routed Port

Working Principle

A physical port on a L3 device can be configured as a routed port, which functions as the gateway interface for L3 switching. The routed port cannot be used for L2 switching. You can run the **no switchport** command to change a switch port to a

routed port and assign an IP address to this port to set up a route. Note that you must delete all L2 features of a switch port before running the **no switchport** command.

1.3.10 L3 AP Port

Working Principle

Like a L3 routed port, you can run the **no switchport** command to change a L2 AP port into a L3 AP port on a L3 device, and then assign an IP address to this AP port to set up a route. Note that you must delete all L2 features of the AP port before running the **no switchport** command.

A L2 AP port with one or more member ports cannot be configured as a L3 AP port. Similarly, a L3 AP port with one or more member ports cannot be changed to a L2 AP port.

1.3.11 Selection of Interface Medium Type

You can select the medium type (fiber or copper) of a combo port as required.

Working Principle

You can choose either fiber or copper as the medium, but the two media cannot take effect at the same time. Once you select the medium, attributes, including the connection status, speed, duplex mode, and flow control mode, are attributes of the selected medium. If you change the medium, the interface will adopt the default settings, and you must re-configure these attributes according to requirements.

The Combo Port Supports Automatic Selection of the Medium Type

- If you enable automatic selection of the medium type, the device uses the current medium if only one medium is available.
- If both media are available, the device uses the preferred medium that is configured. By default, the preferred medium is copper. You can run the **medium-type auto-select prefer fiber** command to configure fiber as the preferred media. In automatic medium selection mode, the interface adopts the default settings of attributes, such as the speed, duplex mode, and flow control mode.

If an interface is enabled with automatic selection, its peer interface must be enabled with auto negotiation; otherwise, an error will occur.

The command takes effect only on a physical port. An AP port or SVI does not support configuration of the medium type.

The command takes effect only on a port that supports medium selection.

All ports that are configured as member ports of an AP port must have the same medium type; otherwise, they cannot be added to the AP port. The type of member ports cannot be modified. A port enabled with automatic medium selection cannot be added to an AP port.

1.3.12 Interface Speed, Duplex Mode

You can configure the interface speed, duplex mode of an Ethernet physical port or AP port.

Working Principle

Speed

Generally, the speed of an Ethernet physical port is determined through negotiation with the peer device. The negotiated speed can be any speed within the interface capability. You can also configure any speed within the interface capability for the Ethernet physical port.

When you configure the speed of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

Duplex Mode

- The duplex mode of an Ethernet physical port or AP port can be configured as follows:
- Set the duplex mode of the interface to full-duplex so that the interface can receive packets while sending packets.
- Set the duplex mode of the interface to half-duplex so that the interface can receive or send packets at a time.
- Set the duplex mode of the interface to auto-negotiation so that the duplex mode of the interface is determined through auto negotiation between the local interface and peer interface.
- When you configure the duplex mode of an AP port, the configuration takes effect on all of its member ports. (All these member ports are Ethernet physical ports.)

1.3.13 Automatic Module Detection

If the interface speed is set to auto, the interface speed can be automatically adjusted based on the type of the inserted module.

Working Principle

Currently, the automatic module detection function can be used to detect only the SFP and SFP+ modules. The SFP is a Gigabit module, whereas SFP+ is a 10 Gigabit module. If the inserted module is SFP, the interface works in Gigabit mode. If the inserted module is SFP+, the interface works in 10 Gigabit mode.

The automatic module detection function takes effect only when the interface speed is set to auto.

1.3.14 Port Errdisable Recovery

Some protocols support the port errdisable recovery function to ensure security and stability of the network. For example, in the port security protocol, when you enable port security and configure the maximum number of security addresses on the port, a port violation event is generated if the number of addresses learned on this port exceeds the maximum number of security addresses. Other protocols, such as the Spanning Tree Protocol (STP), DOT1X, and REUP, support the similar functions, and a violating port will be automatically shut down to ensure security.

Working Principle

After a port is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recovery all the ports in errdisable state and enable these ports. You can manually recover a port, or automatically recover a port at a scheduled time.

1.4 Configuration

Configuration	Description and Command	
Performing Basic Configurations	(Optional) It is used to manage interface configurations, for example, creating/deleting an interface, or configuring the interface description.	
	interface	Creates an interface and enters configuration mode of the created interface or a specified interface.
	interface range	Enters an interface range, creates these interfaces (if not created), and enters interface configuration mode.
	define interface-range	Creates a macro to specify an interface range.
	snmp-server if-index persist	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
	description	Configures the interface description of up to 80 characters in interface configuration mode.
	snmp trap link-status	Configures whether to send the link traps of the interface.
	shutdown	Shuts down an interface in interface configuration mode.
Configuring Interface Attributes	(Optional) It is used to configure interface attributes.	
	bandwidth	Configures the bandwidth of an interface in interface configuration mode.
	carrier-delay	Configures the carrier delay of an interface in interface configuration mode.
	load-interval	Configures the interval for load calculation of an interface.
	duplex	Configures the duplex mode of an interface.
	mtu	Configures the MTU of an interface.
	negotiation mode	Configures the auto negotiation mode of an interface.
	speed	Configures the speed of an interface.
	switchport	Configures an interface as a L2 interface in interface configuration mode. (Run the **no switchport** command to configure an interface as a L3 interface.)
	switchport protected	Configures a port as a protected port.
	errdisable recovery	Recovers a port in errdisable state in global configuration mode.

1.4.1 Performing Basic Configurations

Configuration Effect

- Create a specified logical interface and enter configuration mode of this interface, or enter configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter interface configuration mode, or enter configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description so that users can directly learn information about the interface.
- Enable or disable the link trap function of an interface.
- Enable or disable an interface.

Notes

- The **no** form of the command can be used to delete a specified logical interface or logical interfaces in a specified range, but cannot be used to delete a physical port or physical ports in a specified range.
- The **default** form of the command can be used in interface configuration mode to restore default settings of a specified physical or logical interface, or interfaces in a specified range.

Configuration Steps

↘ Configuring a Specified Interface

- Optional.
- Run this command to create a logical interface or enter configuration mode of a physical port or an existing logical interface.

Command	**interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. The interface can be an Ethernet physical port, AP port, SVI, or loopback interface.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	● If a logical interface is not created yet, run this command to create this interface and enter configuration mode of this interface. ● For a physical port or an existing logical interface, run this command to enter configuration mode of this interface. ● Use the **no** form of the command to delete a specified logical interface. ● Use the **default** form of the command to restore default settings of the interface in interface configuration mode.

↘ Configuring Interfaces Within a Range

- Optional.
- Run this command to create multiple logical interfaces or enter configuration mode of multiple physical port or existing logical interfaces.

Command	**interface range** { *port-range* | **macro** *macro_name* }
Parameter Description	*port-range*: Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical ports, AP ports, SVIs, or loopback interfaces. *macro_name*: Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	• If logical interfaces are not created yet, run this command to create these interfaces and enter interface configuration mode. • For multiple physical ports or existing logical interfaces, run this command to enter interface configuration mode. • Use the **default** form of the command to restore default settings of these interfaces in interface configuration mode. • Before using a macro, run the **define interface-range** command to define the interface range as a macro name in global configuration mode, and then run the **interface range macro** *macro_name* command to apply the macro.

Configuring Interface Index Persistence

- Optional.
- Run this command when the interface indexes must remain unchanged after the device is restarted.

Command	**snmp-server if-index persist**
Parameter Description	N/A
Defaults	By default, interface index persistence is disabled.
Command Mode	Global configuration mode
Usage Guide	After this command is executed, current indexes of all interfaces will be saved, and the indexes remain unchanged after the device is restarted. You can use the **no** or **default** form of the command to disable the interface index persistence function.

Configuring the Description of an Interface

- Optional.
- Run this command to configure the description of an interface.

Command	**description** *string*
Parameter Description	*string:* Indicates a string of up to 80 characters.

Defaults	By default, no description is configured.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the description of an interface. You can use the **no** or **default** form of the command to delete the description of an interface.-

Configuring the Link Trap Function of an Interface

- Optional.
- Run this command to obtain the link traps through SNMP.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, the link trap function is enabled.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the link trap function on an interface. When this function is enabled, the SNMP sends link traps when the link status changes on the interface. You can use the **no** or **default** form of the command to disable the link trap function.

Configuring the Administrative Status of an Interface

- Optional.
- Run this command to enable or disable an interface.
- An interface cannot send or receive packets after it is disabled.

Command	**Shutdown**
Parameter Description	N/A
Defaults	By default, the administrative status of an interface is Up.
Command Mode	Interface configuration mode
Usage Guide	You can run the **shutdown** command to disable an interface, or the **no shutdown** command to enable an interface. In some cases, for example, when an interface is in errdisable state, you cannot run the **no shutdown** command on an interface. You can use the **no** or **default** form of the command to enable the interface.

Verification

Configuring a Specified Interface

- Run the **interface** command. If you can enter interface configuration mode, the configuration is successful.

- For a logical interface, after the **no interface** command is executed, run the **show running** or **show interfaces** command to check whether the logical interface exists. If not, the logical interface is deleted.
- After the **default interface** command is executed, run the **show running** command to check whether the default settings of the corresponding interface are restored. If yes, the operation is successful.

Configuring Interfaces Within a Range

- Run the **interface range** command. If you can enter interface configuration mode, the configuration is successful.
- After the **default interface range** command is executed, run the **show running** command to check whether the default settings of the corresponding interfaces are restored. If yes, the operation is successful.

Configuring Interface Index Persistence

- After the **snmp-server if-index persist** command is executed, run the **write** command to save the configuration, restart the device, and run the **show interface** command to check the interface index. If the index of an interface remains the same after the restart, interface index persistence is enabled.

Configuring the Link Trap Function of an Interface

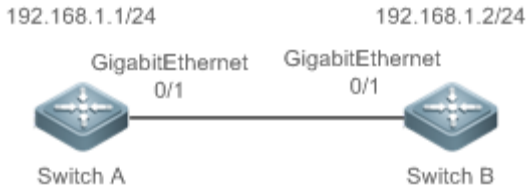
- Remove and then insert the network cable on a physical port, and enable the SNMP server. If the SNMP server receives link traps, the link trap function is enabled.
- Run the **no** form of the **snmp trap link-status** command. Remove and then insert the network cable on a physical port. If the SNMP server does not receive link traps, the link trap function is disabled.

Configuring the Administrative Status of an Interface

- Insert the network cable on a physical port, enable the port, and run the **shutdown** command on this port. If the syslog is displayed on the Console indicating that the state of the port changes to Down, and the indicator on the port is off, the port is disabled. Run the **show interfaces** command, and verify that the interface state changes to Administratively Down. Then, run the **no shutdown** command to enable the port. If the syslog is displayed on the Console indicating that the state of the port changes to Up, and the indicator on the port is on, the port is enabled.

Configuration Example

Configuring Basic Attributes of Interfaces

Scenario **Figure 1-4**	
Configuration Steps	• Connect two devices through the switch ports. • Configure an SVI respectively on two devices, and assign IP addresses from a network segment to the two SVIs.

	● Enable interface index persistence on the two devices. ● Enable the link trap function on the two devices. ● Configure the interface administrative status on the two devices.
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown A(config-if-GigabitEthernet 0/1)# end A# write
B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Verification	Perform verification on Switch A and Switch B as follows: ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether GigabitEthern 0/1 and SVI 1 are Down. ● Run the **shutdown** command on port GigabitEthern 0/1, and check whether a trap indicating that this interface is Down is sent. ● Restart the device, and check whether the index of GigabitEthern 0/1 is the same as that before the restart.
A	A# show interfaces gigabitEthernet 0/1

Index(dec):1 (hex):1

GigabitEthernet 0/1 is administratively down, line protocol is DOWN

Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)

Interface address is: no ip address

MTU 1500 bytes, BW 1000000 Kbit

Encapsulation protocol is Bridge, loopback not set

Keepalive interval is 10 sec, set

Carrier delay is 2 sec

Rxload is 1/255, Txload is 1/255

Queue	Transmitted packets	Transmitted bytes	Dropped packets	Dropped bytes
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	4	440	0	0

Switchport attributes:

interface's description:""

lastchange time:0 Day:20 Hour:15 Minute:22 Second

Priority is 0

admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown

admin speed is AUTO, oper speed is Unknown

flow control admin status is OFF, flow control oper status is Unknown

	admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP, line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) **Interface address is: 192.168.1.1/24** ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b) MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec

Rxload is 1/255, Txload is 1/255

Queue	Transmitted packets	Transmitted bytes	Dropped packets	Dropped bytes
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	4	440	0	0

Switchport attributes:

interface's description:""

lastchange time:0 Day:20 Hour:15 Minute:22 Second

Priority is 0

admin medium-type is Copper, oper medium-type is Copper

admin duplex mode is AUTO, oper duplex is Unknown

admin speed is AUTO, oper speed is Unknown

flow control admin status is OFF, flow control oper status is Unknown

admin negotiation mode is OFF, oper negotiation state is ON

Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF

Port-type: access

Vlan id: 1

10 seconds input rate 0 bits/sec, 0 packets/sec

10 seconds output rate 0 bits/sec, 0 packets/sec

4 packets input, 408 bytes, 0 no buffer, 0 dropped

	Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets B# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP, line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) **Interface address is: 192.168.1.2/24** ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255

1.4.2 Configuring Interface Attributes

Configuration Effect

- Enable the device to connect and communicate with other devices through the switch port or routed port.
- Adjust various interface attributes on the device.

Configuration Steps

↘ Configuring a Routed Port

- Optional.
- Run this command to configure a port as a L3 routed port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.
- This command is applicable to a L2 switch port.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an Ethernet physical port is a L2 switch port.
Command Mode	Interface configuration mode
Usage Guide	On a L3 device, you can run this command to configure a L2 switch port as a L3 routed port. You can run the

	switchport command to change a L3 routed port into a L2 switch port.

Configuring a L3 AP Port

- Optional.
- Run the **no switchport** command in interface configuration mode to configure a L2 AP port as a L3 AP port. Run the **switchport** command to configure a L3 AP port as a L2 AP port.
- After a port is configured as a L3 routed port, L2 protocols running on the port do not take effect.
- This command is applicable to a L2 AP port.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an AP port is a L2 AP port.
Command Mode	Interface configuration mode
Usage Guide	After entering configuration mode of a L2 AP port on a L3 device, you can run this command to configure a L2 AP port as a L3 AP port. After entering configuration mode of a L3 AP port, you can run the **switchport** command to change a L3 AP port into a L2 AP port.

Configuring the Medium Type of an Interface

- Optional.
- By default, the medium type of a combo port is copper.
- Port flapping may occur if the configured medium type of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**medium-type** { **auto-select** [**prefer** [**fiber | copper**]] **| fiber | copper** }
Parameter Description	**auto-select**: Indicates that the medium type is selected automatically. **prefer** [**fiber** | **copper**]: Indicates the medium type that will be preferentially selected. **fiber**: Indicates that fiber is forcibly selected as the medium type. **copper**: Indicates that copper is forcibly selected as the medium type.
Defaults	By default, the medium type of an interface is copper.
Command Mode	Interface configuration mode
Usage Guide	Select either fiber or copper as the medium type of a port when both medium types are available. Once the medium type is selected, all interface attributes, including the status, duplex mode, and speed, are configured for the interface of the selected medium type. If the interface type is changed, the attributes of the new interface type are the default attributes. You can reconfigure these attributes as required. If you enable automatic selection of the medium type, the device uses the current medium if only one medium is available. If both media are available, the device uses the preferred medium as configured. By default, the preferred medium is copper. You can run the **medium-type auto-select prefer fiber** command to configure fiber as the preferred media. In automatic medium selection mode, the interface adopts the default settings of attributes, such as the speed, duplex mode, and flow control mode.

Configuring the Speed of an Interface

- Optional.
- Port flapping may occur if the configured speed of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**speed** [**10** | **100** | **1000** | **auto**]
Parameter Description	**10**: Indicates that the speed of the interface is 10 Mbps. **100**: Indicates that the speed of the interface is 100 Mbps. **1000**: Indicates that the speed of the interface is 1000 Mbps. **auto**: Indicates that the speed of the interface automatically adapts to the actual condition.
Defaults	By default, the speed of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	If an interface is an AP member port, the speed of this interface is determined by the speed of the AP port. When the interface exits the AP port, it uses its own speed configuration. You can run **show interfaces** to display the speed configurations. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of an SFP interface to 10 Mbps.

Configuring the Duplex Mode of an Interface

- Optional.
- Port flapping may occur if the configured duplex mode of a port changes.
- This command is applicable to an Ethernet physical port or AP port.

Command	**duplex** { **auto** | **full** | **half** }
Parameter Description	**auto**: Indicates automatic switching between full duplex and half duplex. **full**: Indicates full duplex. **half**: Indicates half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	The duplex mode of an interface is related to the interface type. You can run **show interfaces** to display the configurations of the duplex mode.

Configuring the MTU of an Interface

- Optional.
- You can configure the MTU of a port to limit the length of a frame that can be received or sent over this port.
- This command is applicable to an Ethernet physical port or SVI.

Command	**mtu** *num*
Parameter Description	*num*: *64–9216*

Defaults	By default, the MTU of an interface is 1500 bytes.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the interface MTU, that is, the maximum length of a data frame at the link layer. Currently, you can configure MTU for only a physical port or an AP port that contains one or more member ports.

Configuring the Bandwidth of an Interface

- Optional.
- Generally, the bandwidth of an interface is the same as the speed of the interface.

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits*: The value ranges from 1 to 2,147,483,647. The unit is kilo bits.
Defaults	Generally, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a gigabit Ethernet physical port is 1,000,000, and that of a 10G Ethernet physical port is 10,000,000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay of an Interface

- Optional.
- If the configured carrier delay is long, it takes a long time to change the protocol status when the physical status of an interface changes. If the carrier delay is set to 0, the protocol status changes immediately after the physical status of an interface changes.

Command	**carrier-delay** *seconds*
Parameter Description	*seconds*: The value ranges from 0 to 60. The unit is second.
Defaults	By default, the carrier delay of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	

Configuring the Load Interval of an Interface

- Optional.
- The configured load interval affects computation of the average packet rate on an interface. If the configured load interval is short, the average packet rate can accurately reflect the changes of the real-time traffic.

Command	**load-interval** *seconds*
Parameter De	*seconds*: The value ranges from 5 to 600. The unit is second.

scription	
Defaults	By default, the load interval of an interface is 10s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Port Errdisable Recovery

- Optional.
- By default, a port will be disabled and will not be recovered after a violation occurs. After port errdisable recovery is configured, a port in errdisable state will be recovered and enabled.

Command	**errdisable recovery [interval** *time***]**
Parameter Description	*time*: Indicates the automatic recovery time. The value ranges from 30 to 86,400. The unit is second.
Defaults	By default, port errdisable recovery is disabled.
Command Mode	Global configuration mode
Usage Guide	By default, a port in errdisable state is not recovered. You can recover the port manually or run this command to automatically recover the port.

Verification

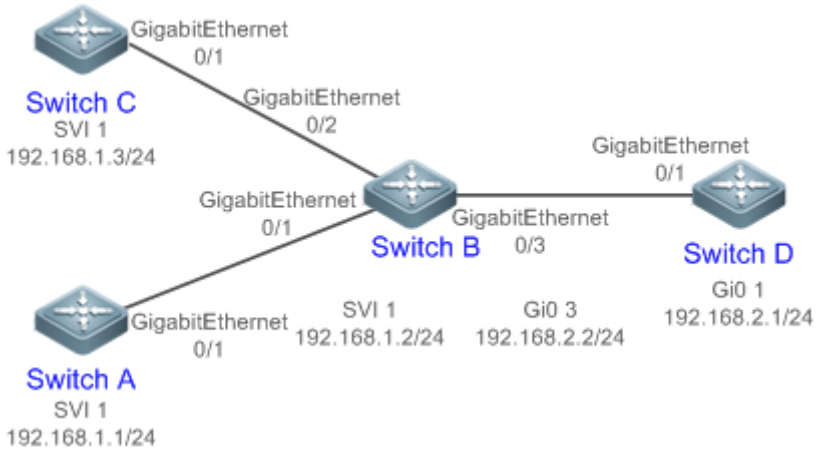
- Run the **show interfaces** command to display the attribute configurations of interfaces.

Command	**show interfaces** [*interface-type interface-number*] [**description | switchport | trunk**]
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. **description**: Indicates the interface description, including the link status. **switchport**: Indicates the L2 interface information. This parameter is effective only for a L2 interface. **trunk**: Indicates the Trunk port information. This parameter is effective for a physical port or an AP port.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command without any parameter to display the basic interface information.
	SwitchA#show interfaces GigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is DOWN, line protocol is DOWN Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b) Interface address is: no ip address Interface IPv6 address is: No IPv6 address MTU 1500 bytes, BW 1000000 Kbit

	Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Medium-type is Copper Admin duplex mode is AUTO, oper duplex is Unknown Admin speed is AUTO, oper speed is Unknown Flow receive control admin status is OFF,flow send control admin status is OFF Flow receive control oper status is Unknown,flow send control oper status is Unknown Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Port-type: trunk Native vlan:1 **Allowed vlan lists:1-4094** //Allowed VLAN list of the Trunk port **Active vlan lists:1, 3-4** //Active VLAN list (indicating that only VLAN 1, VLAN 3, and VLAN 4 are created on the device) Queueing strategy: FIFO Output queue 0/0, 0 drops; Input queue 0/75, 0 drops Rxload is 1/255,Txload is 1/255 5 minutes input rate 0 bits/sec, 0 packets/sec 5 minutes output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 0 packets output, 0 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

Configuration Example

Configuring Interface Attributes

Scenario **Figure 1-1**	
Configuration Steps	● On Switch A, configure GigabitEthernet 0/1 as an access mode, and the default VLAN ID is 1. Configure SVI 1, assign an IP address to SVI 1, and set up a route to Switch D. ● On Switch B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as Trunk ports, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed port, and assign an IP address from another network segment to this port. ● On Switch C, configure GigabitEthernet 0/1 as an Access port, and the default VLAN ID is 1. Configure SVI 1, and assign an IP address to SVI 1. ● On Switch D, configure GigabitEthernet 0/1 as a routed port, assign an IP address to this port, and set up a route to Switch A.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode access A(config-if-GigabitEthernet 0/1)# switchport access vlan 1 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# switchport mode trunk B(config-if-GigabitEthernet 0/1)# exit

	B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# switchport mode trunk B(config-if-GigabitEthernet 0/2)# exit B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)# no switchport B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/3)# exit
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Verification	Perform verification on Switch A, Switch B, Switch C, and Switch D as follows: ● On Switch A, ping the IP addresses of interfaces of the other three switches. Verify that you can access the other three switches on Switch A.. ● Verify that switch B and Switch D can be pinged mutually.

	● Verify that the interface status is correct.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF **Bridge attributes:** **Port-type: access** **Vlan id: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: **Port-type: trunk** **Native vlan: 1** **Allowed vlan lists: 1-4094** **Active vlan lists: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped

	0 output errors, 0 collisions, 0 interface resets
C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP

	Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

1.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the counters of a specified interface.	**clear counters** [*interface-type interface-number*]

Resets the interface hardware.	**clear interface** *interface-type interface-number*

Displaying

Displaying Interface Configurations and Status

Description	Command
Displays all the status and configuration information of a specified interface.	**show interfaces** [*interface-type interface-number*]
Displays the interface status.	**show interfaces** [*interface-type interface-number*] **status**
Displays the interface errdisable status.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Displays the link status change time and count of a specified port.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Displays the administrative and operational states of switch ports (non-routed ports).	**show interfaces** [*interface-type interface-number*] **switchport**
Displays the description and status of a specified interface.	**show interfaces** [*interface-type interface-number*] **description**
Displays the counters of a specified port, among which the displayed speed may have an error of ±0.5%.	**show interfaces** [*interface-type interface-number*] **counters**
Displays the number of packets increased in a load interval.	**show interfaces** [*interface-type interface-number*] **counters increment**
Displays statistics about error packets.	**show interfaces** [*interface-type interface-number*] **counters error**
Displays the packet sending/receiving rate of an interface.	**show interfaces** [*interface-type interface-number*] **counters rate**
Displays a summary of interface information.	**show interfaces** [*interface-type interface-number*] **counters summary**
Displays the bandwidth usage of an interface.	**show interfaces** [*interface-type interface-number*] **usage**

2 Configuring MAC Address

2.1 Overview

A MAC address table contains the MAC addresses, interface numbers and VLAN IDs of the devices connected to the local device.

When a device forwards a packet, it finds an output port from its MAC address table according to the destination MAC address and the VLAN ID of the packet.

After that, the packet is unicast, multicast or broadcast.

This document covers dynamic MAC addresses, static MAC addresses and filtered MAC addresses. For the management of multicast MAC addresses, please see *Configuring IGMP Snooping Configuration*.

Protocols and Standards

- IEEE 802.3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q: Virtual Bridged Local Area Networks

2.2 Applications

Application	Description
MAC Address Learning	Forward unicast packets through MAC addresses learning.
MAC Address Change Notification	Monitor change of the devices connected to a network device through MAC address change notification.

2.2.1 MAC Address Learning

Scenario

Usually a device maintains a MAC address table by learning MAC addresses dynamically. The operating principle is described as follows:

As shown in the following figure, the MAC address table of the switch is empty. When User A communicates with User B, it sends a packet to the port GigabitEthernet 0/2 of the switch, and the switch learns the MAC address of User A and stores it in the table.
As the table does not contain the MAC address of User B, the switch broadcasts the packet to the ports of all connected devices except User A, including User B and User C.

Figure 2-1 Step 1 of MAC Address Learning

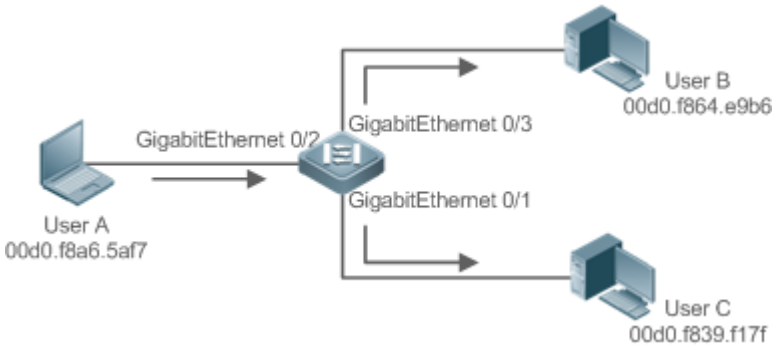


Figure 2-2 MAC Address Table 1

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

When User B receives the packet, it sends a reply packet to User A through port GigabitEthernet 0/3 on the switch. As the MAC address of User A is already in the MAC address table, the switch send the reply unicast packet to port GigabitEthernet 0/2 port and learns the MAC address of User B. User C does not receive the reply packet from User B to User A.

Figure 2-3 Step 2 of MAC Address Learning

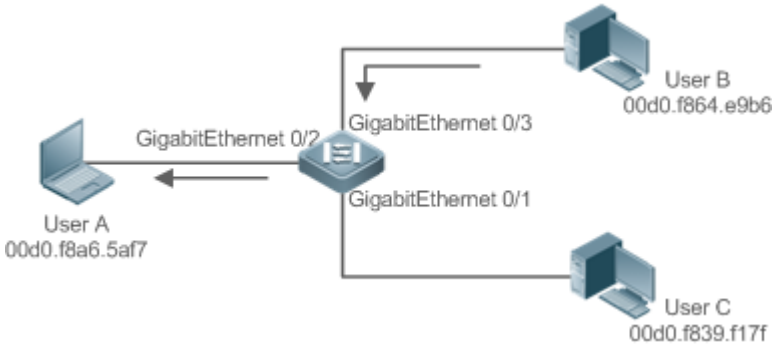


Figure 2-4 MAC Address Table 2

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

Through the interaction between User A and User B, the switch learns the MAC addresses of User A and User B. After that, packets between User A and User B will be exchanged via unicast without being received by User C.

Deployment

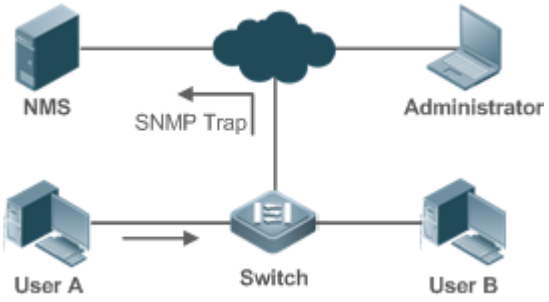
- With MAC address learning, a layer-2 switch forwards packets through unicast, reducing broadcast packets and network load.

2.2.2 MAC Address Change Notification

MAC address change notification provides a mechanism for the network management system (NMS) to monitor the change of devices connected to a network device.

Scenario

Figure 2-5 MAC Address Change Notification



After MAC address change notification is enabled on a device, the device generates a notification message when the device learns a new MAC address or finishes aging a learned MAC address, and sends the message in an SNMP Trap message to a specified NMS.

A notification of adding a MAC address indicates that a new user accesses the network, and that of deleting a MAC address indicates that a user sends no packets within an aging time and usually the user exits the network.

When a network device is connected to a number of devices, a lot of MAC address changes may occur in a short time, resulting in an increase in traffic. To reduce traffic, you may configure an interval for sending MAC address change notifications. When the interval expires, all notifications generated during the interval are encapsulated into a message.

±When a notification is generated, it is stored in the table of historical MAC address change notifications. The administrator may know recent MAC address changes by checking the table of notification history even without NMS.

A MAC address change notification is generated only for a dynamic MAC address.

Deployment

- Enable MAC address change notification on a layer-2 switch to monitor the change of devices connected to a network device.

2.3 Features

Basic Concepts

Dynamic MAC Address

A dynamic MAC address is a MAC address entry generated through the process of MAC address learning by a device.

Address Aging

A device only learns a limited number of MAC addresses, and inactive entries are deleted through address aging.

A device starts aging a MAC address when it learns it. If the device receives no packet containing the source MAC address, it will delete the MAC address from the MAC address table when the time expires.

Forwarding via Unicast

If a device finds in its MAC address table an entry containing the MAC address and the VLAN ID of a packet and the output port is unique, it will send the packet through the port directly.

Forwarding via Broadcast

If a device receives a packet containing the destination address ffff.ffff.ffff or an unidentified destination address, it will send the packet through all the ports in the VLAN where the packet is from, except the input port.

2.4 Configuration

Configuration	Description and Command	
Configuring Dynamic MAC Address	(Optional) It is used to enable MAC address learning.	
	mac-address-learning	Configures MAC address learning globally or on an interface.
	mac-address-table aging-time	Configures an aging time for a dynamic MAC address.
Configuring a Static MAC Address	(Optional) It is used to bind the MAC address of a device with a port of a switch.	
	mac-address-table static	Configures a static MAC address.
Configuring a MAC Address for Packet Filtering	(Optional) It is used to filter packets.	
	mac-address-table filtering	Configures a MAC address for packet filtering.
Configuring MAC Address Change Notification	(Optional) It is used to monitor change of devices connected to a network device.	
	mac-address-table notification	Configures MAC address change notification globally.
	snmp trap mac-notification	Configures MAC address change notification on an interface.

2.4.1 Configuring Dynamic MAC Address

Configuration Effect

Learn MAC addresses dynamically and forward packets via unicast.

Configuration Steps

Configuring MAC Address Learning on Interface

- Optional.
- You can perform this configuration to disable MAC address learning on an interface.

Command	**mac-address-learning**
Parameter Description	**N/A**
Defaults	MAC address learning is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	Perform this configuration on a layer-2 interface, for example, a switch port or an AP port.

By default, MAC address learning is enabled. If DOT1X, IP SOURCE GUARD, or a port security function is configured on a port, MAC address learning cannot be enabled. Access control cannot be enabled on a port with MAC address learning disabled.

Configuring an Aging Time for a Dynamic MAC Address

- Optional.
- Configure an aging time for dynamic MAC addresses.

Command	**mac-address-table aging-time** *value*
Parameter Description	*value*: Indicates the aging time. The value is either 0 or in the range from 10 to 1000,000.
Defaults	The default is 300s.
Command Mode	Global configuration mode
Usage Guide	If the value is set to 0, MAC address aging is disabled and learned MAC addresses will not be aged.

The actual aging time may be different from the configured value, but it is not more than two times of the configured value.

Verification

- Check whether a device learns dynamic MAC addresses.
- Run the **show mac-address-table dynamic** command to display dynamic MAC addresses.
- Run the **show mac-address-table aging-time** command to display the aging time for dynamic MAC addresses.

Command	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Displays the information of a specific dynamic MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port.

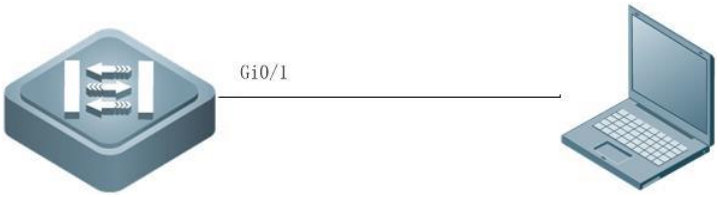
	vlan *vlan-id*: Displays the dynamic MAC addresses in a specific VLAN.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
	Ruijie# show mac-address-table dynamic Vlan MAC Address Type Interface ---- ---------- ------ ---------- **1 0000.0000.0001 DYNAMIC GigabitEthernet 1/1** **1 0001.960c.a740 DYNAMIC GigabitEthernet 1/1** **1 0007.95c7.dff9 DYNAMIC GigabitEthernet 1/1** **1 0007.95cf.eee0 DYNAMIC GigabitEthernet 1/1** **1 0007.95cf.f41f DYNAMIC GigabitEthernet 1/1** **1 0009.b715.d400 DYNAMIC GigabitEthernet 1/1** **1 0050.bade.63c4 DYNAMIC GigabitEthernet 1/1**

Field	Description
Vlan	Indicates the VLAN where the MAC address resides.
MAC Address	Indicates a MAC Address.
Type	Indicates a MAC address type.
Interface	Indicates the interface where the MAC address resides.

Command	**show mac-address-table aging-time**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A
	Ruijie# show mac-address-table aging-time **Aging time: 300**

Configuration Example

Configuring Dynamic MAC Address

Scenario **Figure 2-6**	
Configuration Steps	● Enable MAC address learning on an interface. ● Configure the aging time for dynamic MAC addresses to 180s. ● Delete all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Ruijie# configure terminal Ruijie(config-if-GigabitEthernet 0/1)# mac-address-learning Ruijie(config-if-GigabitEthernet 0/1)# exit Ruijie(config)# mac aging-time 180 Ruijie# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Verification	● Check MAC address learning on an interface. ● Display the aging time for dynamic MAC addresses. ● Display all dynamic MAC addresses in VLAN 1 on port GigabitEthernet 0/1.
	Ruijie# show mac-address-learning **GigabitEthernet 0/1 learning ability: enable** Ruijie# show mac aging-time Aging time : **180 seconds** Ruijie# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1 Vlan MAC Address Type Interface ---------- -------------------- -------- -------------------- **1 00d0.f800.1001 STATIC GigabitEthernet 1/1**

Common Errors

Configure MAC address learning on an interface before configuring the interface as a layer-2 interface, for example, a switch port or an AP port.

2.4.2 Configuring a Static MAC Address

Configuration Effect

- Bind the MAC address of a network device with a port of a switch.

Configuration Steps

Configuring a Static MAC address

- Optional.
- Bind the MAC address of a network device with a port of a switch.

Command	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides. **interface** *interface-id*: Specifies a physical interface or an AP port.
Defaults	By default, no static MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	When the switch receives a packet containing the specified MAC address on the specified VLAN, the packet is forwarded to the bound interface.

Verification

- Run the **show mac-address-table static** command to check whether the configuration takes effect.

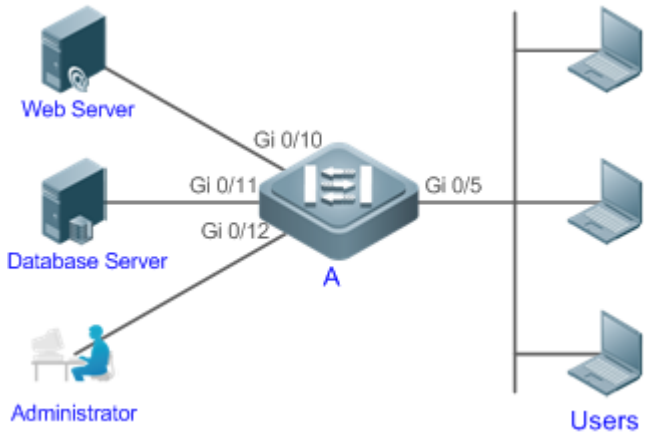
Command	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Specifies a MAC address. **interface** *interface-id*: Specifies a physical interface or an AP port. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	Ruijie# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ------------------ **1 00d0.f800.1001 STATIC GigabitEthernet 1/1** **1 00d0.f800.1002 STATIC GigabitEthernet 1/1** **1 00d0.f800.1003 STATIC GigabitEthernet 1/1**

Configuration Example

Configuring a Static MAC address

In the above example, the relationship of MAC addresses, VLAN and interfaces is shown in the following table.

Role	MAC Address	VLAN ID	Interface ID
Web Server	00d0.3232.0001	VLAN2	Gi0/10
Database Server	00d0.3232.0002	VLAN2	Gi0/11

Administrator	00d0.3232.1000	VLAN2	Gi0/12
Scenario **Figure 2-7**			
Configuration Steps	● Specify destination MAC addresses (*mac-address*). ● Specify the VLAN (*vlan-id*) where the MAC addresses reside. ● Specify interface IDs (*interface-id*).		
A	A# configure terminal A(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2 interface gigabitEthernet 0/10 A(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2 interface gigabitEthernet 0/11 A(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2 interface gigabitEthernet 0/12		
Verification	Display the static MAC address configuration on a switch.		
A	A# show mac-address-table static Vlan MAC Address Type Interface ---------- ---------- -------- ---------- **2 00d0.f800.3232.0001 STATIC GigabitEthernet 0/10** **2 00d0.f800.3232.0002 STATIC GigabitEthernet 0/11** **2 00d0.f800.3232.1000 STATIC GigabitEthernet 0/12**		

Common Errors

- Configure a static MAC address before configuring the specific port as a layer-2 interface, for example, a switch port or an AP port.

2.4.3 Configuring a MAC Address for Packet Filtering

Configuration Effect

- If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Configuration Steps

Configuring a MAC Address for Packet Filtering

- Optional.
- Perform this configuration to filter packets.

Command	**mac-address-table filtering** *mac-address* **vlan** *vlan-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Defaults	By default, no filtered MAC address is configured.
Command Mode	Global configuration mode
Usage Guide	If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Verification

- Run the **show mac-address-table filter** command to display the filtered MAC address.

Command	**show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
	Ruijie# show mac-address-table filtering Vlan MAC Address Type Interface ------ -------------------- -------- ----------- **1 0000.2222.2222 FILTER**

Configuration Example

Configuring a MAC Address for Packet Filtering

Configuration Steps	● Specify a destination MAC address (*mac-address*) for filtering. ● Specify a VLAN where the MAC addresses resides.
	Ruijie# configure terminal Ruijie(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1

Verification	Display the filtered MAC address configuration.
	Ruijie# show mac-address-table filter Vlan MAC Address Type Interface ---------- -------------------- -------- -------------------- **1 00d0.f800.3232.0001 FILTER**

2.4.4 Configuring MAC Address Change Notification

Configuration Effect

- Monitor change of devices connected to a network device.

Configuration Steps

Configuring NMS

- Optional.
- Perform this configuration to enable an NMS to receive MAC address change notifications.

Command	**snmp-server host** *host-addr* **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*
Parameter Description	**host** *host-addr*: Specifies the IP address of a receiver. **version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: Specifies the version of SNMP TRAP messages. You can also specify authentication and a security level for packets of Version 3. *community-string*: Indicates an authentication name.
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling SNMP Trap

- Optional.
- Perform this configuration to send SNMP Trap messages.

Command	**snmp-server enable traps**
Parameter Description	N/A
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Global MAC Address Change Notification

- Optional.
- If MAC address change notification is disabled globally, it is disabled on all interfaces.

Command	**mac-address-table notification**
Parameter Description	N/A
Defaults	By default, MAC address change notification is disabled globally.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring MAC Address Change Notification On Interface

- Optional.
- Perform this configuration to enable MAC address change notification on an interface.

Command	**snmp trap mac-notification** { **added** | **removed** }
Parameter Description	**added**: Generates a notification when an MAC address is added. **removed**: Generates a notification when an MAC address is deleted.
Defaults	By default, MAC address change notification is disabled on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Interval for Generating MAC Address Change Notifications and Volume of Notification History

- Optional.
- Perform this configuration to modify the interval for generating MAC address change notifications and the volume of notification history.

Command	**mac-address-table notification** { **interval** *value* | **history-size** *value* }
Parameter Description	**interval** *value*: (Optional) Indicates the interval for generating MAC address change notifications. The value ranges from 1 to 3600 seconds,. **history-size** *value*: Indicates the maximum number of entries in the table of notification history. The value ranges from 1 to 200.
Defaults	The default interval is 1 second. The default maximum amount of notifications is 50.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

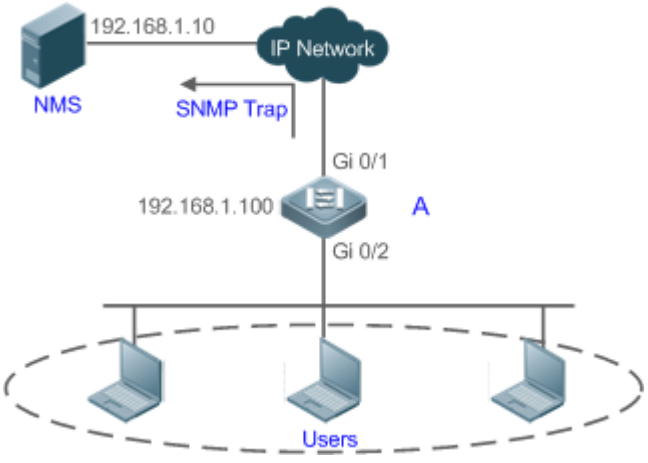
- Run the **show mac-address-table notification** command to check whether the NMS receives MAC address change notifications.

Command	**show mac-address-table notification [interface [*interface-id*] | history]**
Parameter Description	**Interface**:Displays the configuration of MAC address change notification on all interfaces. ***interface-id***: Displays the configuration of MAC address change notification on a specified interface. **history**: Displays the history of MAC address change notifications.
Command Mode	Privileged EXEC mode/Global configuration mode /Interface configuration mode
Usage Guide	N/A
Usage Guide	Display the configuration of global MAC address change notification. Ruijie#show mac-address-table notification MAC Notification Feature : **Enabled** Interval(Sec): **300** Maximum History Size : **50** Current History Size : **0**

Field	Description
Interval(Sec)	Indicates the interval for generating MAC address change notifications.
Maximum History Size	Indicates the maximum number of entries in the table of notification history.
Current History Size	Indicates the current notification entry number.

Configuration Example

Scenario
Figure 2-8



The figure shows an intranet of an enterprise. Users are connected to A via port Gi0/2.

The Perform the configuration to achieve the following effects:

	● When port Gi0/2 learns a new MAC address or finishes aging a learned MAC address, a MAC address change notification is generated. ● Meanwhile, A sends the MAC address change notification in an SNMP Trap message to a specified NMS. ● In a scenario where A is connected to a number of Users, the configuration can prevent MAC address change notification burst in a short time so as to reduce the network flow.
Configuration Steps	● Enable global MAC address change notification on A, and configure MAC address change notification on port Gi0/2. ● Configure the IP address of the NMS host, and enable A with SNMP Trap. A communicates with the NMS via routing. ● Configure the interval for sending MAC address change notifications to 300 seconds (1 second by default).
A	Ruijie# configure terminal Ruijie(config)# mac-address-table notification Ruijie(config)# interface gigabitEthernet 0/2 Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed Ruijie(config-if-GigabitEthernet 0/2)# exit Ruijie(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 Ruijie(config)# snmp-server enable traps Ruijie(config)# mac-address-table notification interval 300
Verification	● Check t whether MAC address change notification is enabled globally . ● Check whether MAC address change notification is enabled on the interface. ● Display the MAC addresses of interfaces, and run the **clear mac-address-table dynamic** command to simulate aging dynamic MAC addresses. ● Check whether global MAC address change notification is enabled globally. ● Display the history of MAC address change notifications.
A	Ruijie# show mac-address-table notification MAC Notification Feature : **Enabled** Interval(Sec): **300** Maximum History Size : **50** Current History Size : **0** Ruijie# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap

	---------- ---------- ---------- GigabitEthernet 0/2 Enabled Enabled Ruijie# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ---------- -------------------- -------- -------------------- 1 00d0.3232.0001 DYNAMIC GigabitEthernet 0/2 Ruijie# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 Ruijie# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683 MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2

Common Errors

None

2.5 Monitoring

Clearing

Running the clear commands may lose vital information and interrupt services.

Description	Command
Clears dynamic MAC addresses.	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

Displaying

Description	Command
Displays the MAC address table.	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address* **]** [**interface** *interface-id*] [**vlan** *vlan-id*]
Displays the aging time for dynamic MAC addresses.	**show mac-address-table aging-time**

Displays the configuration and history of MAC address change notifications.	**show mac-address-table notification [interface [*interface-id*] | history]**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs MAC address operation.	**debug bridge mac**

3 Configuring Aggregated Port

3.1 Overview

An aggregated port (AP) is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

An AP port supports load balancing, namely, distributes load evenly among member links. Besides, an AP port realizes link backup. When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

For example, the link between two devices supports a maximum bandwidth of 1,000 Mbps. When the service traffic carried by the link exceeds 1,000 Mbps, the traffic in excess will be discarded. Port aggregation can be used to solve the problem. For example, you can connect the two devices with network cables and combine multiple links to form a logical link capable of multiples of 1,000 Mbps.

For example, there are two devices connected by a network cable. When the link between the two ports of the devices is disconnected, the services carried by the link will be interrupted. After the connected ports are aggregated, the services will not be affected as long as one link remains connected.

Protocols and Standards

- IEEE 802.3ad

3.2 Applications

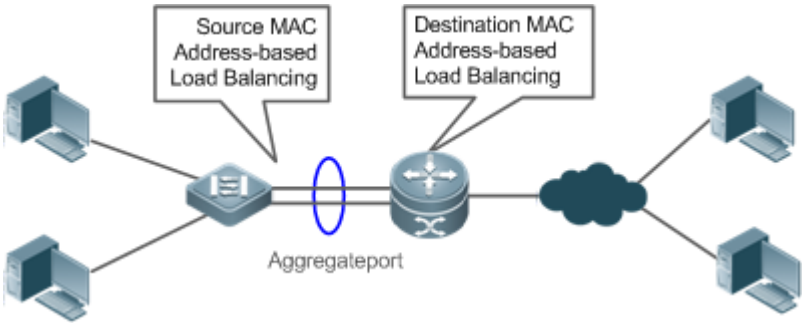
Applications	Description
AP Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires a greater bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase the link bandwidth, and configure a proper load balancing algorithm to distribute the work load evenly to each physical link, thus improving bandwidth utilization.

3.2.1 AP Link Aggregation and Load Balancing

Scenario

In Figure 1-1, the switch communicates with the router through an AP port. All the devices on the intranet (such as the two PCs on the left) use the router as a gateway. All the devices on the extranet (such as the two PCs on the right) send packets to the internet devices through the router, with the gateway's MAC address as its source MAC address. To distribute the load between the router and other hosts to other links, configure destination MAC address-based load balancing. On the switch, configure source MAC address-based load balancing.

Figure 3-1 AP Link Aggregation and Load Balancing



Deployment

- Configure the directly connected ports between the switch and router as a static AP port or a Link Aggregation Control Protocol (LACP) AP port.
- On the switch, configure a source MAC address-based load balancing algorithm.
- On the router, configure a destination MAC address-based load balancing algorithm.

3.3 Features

Basic Concepts

Static AP

The static AP mode is an aggregation mode in which physical ports are directly added to an AP aggregation group through manual configuration to allow the physical ports to forward packets when the ports are proper in link state and protocol state.

An AP port in static AP mode is called a static AP, and its member ports are called static AP member ports.

LACP

LACP is a protocol about dynamic link aggregation. It exchanges information with the connected device through LACP data units (LACPDUs).

An AP port in LACP mode is called an LACP AP port, and its member ports are called LACP AP member ports.

AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member ports in active mode initiate LACP negotiation. AP member ports in passive mode only respond to received LACPDUs. AP member ports in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer port mode.

Port Mode	Peer Port Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static Mode	Static Mode

AP Member Port State

There are two kinds of AP member port state available:

- When a member port is Down, the port cannot forward packets. The Down state is displayed.
- When a member port is Up and the link protocol is ready, the port can forward packets. The Up state is displayed.

There are three kinds of LACP member port state:

- When the link of a port is Down, the port cannot forward packets. The Down state is displayed.
- When the link of a port is Up and the port is added to an aggregation group, the bndl state is displayed.
- When the link of a port is Up but the port is suspended because the peer end is not enabled with LACP or the attributes of the ports are inconsistent with those of the master port, the susp state is displayed. (The port in susp state does not forward packets.)

Only full-duplex ports are capable of LACP aggregation.

LACP aggregation can be implemented only when the rates, flow control approaches, medium types, and Layer-2/3 attributes of member ports are consistent.

If you modify the preceding attributes of a member port in the aggregation group, LACP aggregation will fail.

The ports which are prohibited from joining or exiting an AP port cannot be added to or removed from a static AP port or an LACP AP port.

LACP System ID

One device can be configured with only one LACP aggregation system. The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with an ID of a higher priority determines the port state. The port state of a system with an ID of a lower priority keeps consistent with that of a higher priority.

LACP Port ID

Each port has an independent LACP port priority, which is a configurable value. The port ID consists of the LACP port priority and port number. A smaller port priority indicates a higher priority of the port ID. If the port priorities are the same, a smaller port number indicates a higher priority of the port ID.

LACP Master Port

When dynamic member ports are Up, LACP selects one of those ports to be the master port based on the rates and duplex modes, ID priorities of the ports in the aggregation group, and the bundling state of the member ports in the Up state. Only the ports that have the same attributes as the master port are in Bundle state and participate in data forwarding. When the attributes of ports are changed, LACP reselects a master port. When the new master port is not in Bundle state, LACP disaggregates the member ports and performs aggregation again.

LACP Independent Ports

In normal cases, LACP independent ports are used for interworking between access switches and servers with two NICs. If the OS is not pre-installed when a server with two NICs starts, the OS needs to be installed via the remote PXE OS installation device. Before the OS is installed, the server with two NICs cannot perform LACP negotiation with the access device, and only one NIC can work. In this case, the port on the access device must be able to change to a common Ethernet physical port automatically to ensure normal communication between the server and the remote PXE OS installation device. After the OS is installed and both NICs can run the LACP, the port on the access device must be able to enable the LACP again for negotiation.

LACP independent ports can work only at layer 2. After an LACP independent port is enabled, if the LACP independent port does not receive LACP packets, it automatically changes to a common Ethernet port, which automatically copies the rate, duplex mode, flow control, and VLAN configuration from the AP port to ensure port forwarding capabilities.

An LACP independent port automatically changes to a common Ethernet port only if it does not receive LACP packets within 90s. After the port receives LACP packets, it changes to an LACP member port again.

Overview

Overview	Description
Link Aggregation	Aggregates physical links statically or dynamically to realize bandwidth extension and link backup.
Load Balancing	Balances the load within an aggregation group flexibly by using different load balancing methods.

3.3.1 Link Aggregation

Working Principle

There are two kinds of AP link aggregation. One is static AP, and the other is dynamic aggregation through LACP.

- Static AP

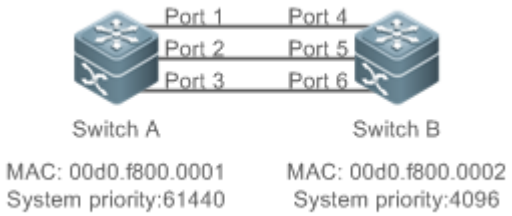
The static AP configuration is simple. Run a command to add the specified physical port to the AP port. After joining the aggregation group, a member port can receive and transmit data and participate in load balancing within the group.

- Dynamic AP (LACP)

An LACP-enabled port sends LACPDUs to advertise its system priority, system MAC address, port priority, port number, and operation key. When receiving the LACPDU from the peer end, the device compares the system priorities of both ends based on the system ID in the packet. The end with a higher system ID priority sets the ports in the aggregation group to Bundle state based on the port ID priorities in a descending order, and sends an updated LACPDU. When receiving the LACPDU, the peer end sets corresponding ports to Bundle state so that both ends maintain consistency when a port exits or joins the aggregation group. The physical link can forward packets only after the ports at both ends are bundled dynamically.

After link aggregation, the LACP member ports periodically exchange LACPDUs. When a port does not receive an LACPDU in the specified time, a timeout occurs and the links are unbundled. In this case, the member ports cannot forward packets. There are two timeout modes: long timeout and short timeout. In long timeout mode, a port sends a packet every 30s. If it does not receive a packet from the peer end in 90s, a timeout occurs. In short timeout mode, a port sends a packet every 1s. If it does not receive a packet from the peer end in 3s, a timeout occurs.

Figure 3-1 LACP Negotiation



In Figure 1-2, Switch A is connected to Switch B through three ports. Set the system priorities of Switch A and Switch B to 61440 and 4096 respectively. Enable LACP on the Ports 1–6, set the aggregation mode to the active mode, and set the port priority to the default value 32768.

When receiving an LACPDU from Switch A, Switch B finds that it has a higher system ID priority than Switch A (the system priority of Switch B is higher than that of Switch A). Switch B sets Port 4, Port 5, and Port 6 to Bundle state based on the order of port ID priorities (or in an ascending order of port numbers if the port priorities are the same). When receiving an updated LACPDU from Switch B, Switch A finds that Switch B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to Bundle state. Then Switch A also sets Port 1, Port 2, and Port 3 to Bundle state.

3.3.2 Load Balancing

Working Principle

AP ports segregate packet flows by using load balancing algorithms based on packet features, such as the source and destination MAC addresses, source and destination IP addresses, and Layer-4 source and destination port numbers. The packet flow with the consistent feature is transmitted by one member link, and different packet flows are evenly distributed to member links. For example, in source MAC address-based load balancing, packets are distributed to the member links based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed to member links. Packets with the identical source MAC address are forwarded by one member link.

Currently, there are several AP load balancing modes as follows:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Layer-4 source port number or Layer-4 destination port number
- Layer-4 source port number + Layer-4 destination port number
- Source IP address + Layer-4 source port number
- Source IP address + Layer-4 destination port number
- Destination IP address + Layer-4 source port number
- Destination IP address + Layer-4 destination port number
- Source IP address + Layer-4 source port number + Layer-4 destination port number

- Destination IP address + Layer-4 source port number + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number
- Source IP address + destination IP address + Layer-4 destination port number
- Source IP address + destination IP address + Layer-4 source port number + Layer-4 destination port number

Load balancing based on IP addresses or port numbers is applicable only to Layer-3 packets. When a device enabled with this load balancing method receives Layer-2 packets, it automatically switches to the default load balancing method.

All the load balancing methods use a load algorithm (hash algorithm) to calculate the member links based on the input parameters of the methods. The input parameters include the source MAC address, destination MAC address, source MAC address + destination MAC address, source IP address, destination IP address, source IP address + destination IP addresses, source IP address + destination IP address + Layer-4 port number and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two packets with different source and destination IP addresses may be distributed to the same member link through calculation.

3.3.3 Wireless AP Aggregated Port

Working Principle

If the wireless traffic exceeds gigabit, a single wired port cannot meet the requirements. In this case, an aggregated port needs to be used for load balancing and bandwidth increasing. Wireless APs adopts the dual uplink deployment mode. If a network cable is disconnected, the other cable can continue to work, ensuring link backup. Aggregated port configuration of wireless APs is delivered by the AC or aggregated ports are configured independently on the APs. If wireless APs work in fit AP mode, aggregated port configuration is delivered by the AC. If wireless APs work in fat AP mode, aggregated ports are configured on the AP console over serial ports.

3.4 Configuration

Configuration	Description and Command	
Configuring Static AP Ports	(Mandatory) It is used to configure link aggregation manually.	
	interface aggregateport	Creates an Ethernet AP port.
	port-group	Configures static AP member ports.
Configuring LACP AP Ports	(Mandatory) It is used to configure link aggregation dynamically.	
	port-group mode	Configures LACP member ports.
	lacp system-priority	Configures the LACP system priority.
	lacp port-priority	Configures the port priority.
	lacp short-timeout	Configures the short timeout mode on a port.

Configuration	Description and Command	
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	snmp trap link-status	Enables LinkTrap advertisement for an AP port.
	aggregateport member linktrap	Enables LinkTrap t for AP member ports.
Configuring a Load Balancing Mode	(Optional) It is used to configure a load balancing mode for an aggregated link.	
	aggregateport load-balance	Configures a load balancing algorithm for an AP port or AP member ports.
Configuring Aggregated Port Configuration Delivery from the AC	**ap-interface wireport** *portnumber* **port-group** *apnumber*	Configures aggregated port configuration delivery from the AC.

3.4.1 Configuring Static AP Ports

Configuration Effect

- Configure multiple physical ports as AP member ports to realize link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical ports can be added to an AP port.
- The ports of different media types or port modes cannot be added to the same AP port.
- Layer-2 ports can be added to only a Layer-2 AP port, and Layer-3 ports can be added to only a Layer-3 AP port. The Layer-2/3 attributes of an AP port that contains member ports cannot be modified.
- After a port is added to an AP port, the attributes of the port are replaced by those of the AP port.
- After a port is removed from an AP port, the attributes of the port are restored.

After a port is added to an AP port, the attributes of the port are consistent with those of the AP port. Therefore, do not perform configuration on the AP member ports or apply configuration to a specific AP member port. However, some configurations (the **shutdown** and **no shutdown** commands) can be configured on AP member ports. When you use AP member ports, check whether the function that you want to configure can take effect on a specific AP member port, and perform this configuration properly.

Configuration Steps

Creating an Ethernet AP Port

- Mandatory.
- Perform this configuration on an AP-enabled device.

Command	**interface aggregateport** *ap-number*
Parameter Description	*ap-number*: Indicates the number of an AP port.
Defaults	By default, no AP port is created.
Command Mode	Global configuration mode
Usage Guide	To create an Ethernet AP port, run **interfaces aggregateport** in global configuration mode. To delete the specified Ethernet AP port, run **no interfaces aggregateport** *ap-number* in global configuration mode.

Run **port-group** to add a physical port to a static AP port in interface configuration mode. If the AP port does not exist, it will be created automatically.

The AP feature must be configured on the devices at both ends of a link and the AP mode must be the same (static AP or LACP AP).

Configuring Static AP Member Ports

- Mandatory.
- Perform this configuration on AP-enabled devices.

Command	**port-group** *ap-number*
Parameter Description	**port-group** *ap-number*: Indicates the number of an AP port.
Defaults	By default, no ports are added to any static AP port.
Command Mode	Interface configuration mode of the specified Ethernet port
Usage Guide	To add member ports to an AP port, run **port-group** in interface configuration mode. To remove member ports from an AP port, run **no port-group** in interface configuration mode.

The static AP member ports configured on the devices at both ends of a link must be consistent.

After a member port exits the AP port, the default settings of the member port are restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an AP port.

After a member port exits an AP port, the port is disabled by using the **shutdown** command to avoid loops. After you confirm that the topology is normal, run **no shutdown** in interface configuration mode to enable the port again.

Converting Layer-2 APs to Layer-3 APs

- Optional.
- When you need to enable Layer-3 routing on an AP port, for example, to configure IP addresses or static route entries, convert the Layer-2 AP port to a Layer-3 AP port and enable routing on the Layer-3 AP port.
- Perform this configuration on AP-enabled devices that support Layer-2 and Layer-3 features, such as Layer-3 switches or wireless access controllers (ACs).

Command	**no switchport**

Parameter Description	N/A
Defaults	By default, the AP ports are Layer-2 AP ports.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	The Layer-3 AP feature is supported by only Layer-3 devices.

The AP port created on a Layer-3 device that does not support Layer-2 feature is a Layer-3 AP port. Otherwise, the AP port is a Layer-2 AP port.

Verification

- Run **show running** to display the configuration.
- Run **show aggregateport summary** to display the AP configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance | summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on all AP ports is displayed if you do not specify the AP port number.
	Ruijie# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring an Ethernet Static AP Port

Scenario **Figure 3-2**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3

Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3
Verification	● Run **show aggregateport summary** to check whether AP port 3 contains member ports GigabitEthernet 1/1 and GigabitEthernet 1/2.
Switch A	SwitchA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi1/1,Gi1/2**
Switch B	SwitchB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag3** 8 Enabled ACCESS **Gi2/1,Gi2/2**

3.4.2 Configuring LACP AP Ports

Configuration Effect

- Connected devices perform autonegotiation through LACP to realize dynamic link aggregation.
- The bandwidth of the aggregation link is equal to the sum of the member link bandwidths.
- When a member link of the AP port is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.

Notes

- After a port exits an LACP AP port, the default settings of the port may be restored. Different functions deal with the default settings of the member ports differently. It is recommended that you check and confirm the port settings after a member port exits an LACP AP port.
- Changing the LACP system priority may cause LACP member ports to be disaggregated and aggregated again.
- Changing the priority of an LACP member port may cause the other member ports to be disaggregated and aggregated again.

Configuration Steps

↘ **Configuring LACP Member Ports**

- Mandatory.

- Perform this configuration on LACP-enabled devices.

Command	**port-group** *key-number* **mode** { **active | passive** }
Parameter Description	*Key-number*: Indicates the management key of an AP port. In other words, it is the LACP AP port number. The maximum value is subject to the number of AP ports supported by the device. **active**: Indicates that ports are added to a dynamic AP port actively. **passive**: Indicates that ports are added to a dynamic AP port passively.
Defaults	By default, no physical ports are added to any LACP AP port.
Command Mode	Interface configuration mode of the specified physical port
Usage Guide	Use this command in interface configuration mode to add member ports to an LACP AP port.

The LACP member port configuration at both ends of a link must be consistent.

Configuring the LACP System Priority

- Optional.
- Perform this configuration when you need to adjust the system ID priority. A smaller value indicates a higher system ID priority. The device with a higher system ID priority selects an AP port.
- Perform this configuration on LACP-enabled devices.

Command	**lacp system-priority** *system-priority*
Parameter Description	*system-priority*: Indicates the LACP system priority. The value ranges from 0 to 65535.
Defaults	By default, the LACP system priority is 32768.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to configure the LACP system priority. All the dynamic member links share one LACP system priority. Changing the LACP system priority will affect all member links. To restore the default settings, run **no lacp system-priority** in interface configuration mode.

Configuring the Priority of an LACP Member Port

- Optional.
- Perform this configuration when you need to specify the port ID priority. A smaller value indicates a higher port ID priority. The port with the highest port ID priority will be selected as the master port.
- Perform this configuration on LACP-enabled devices.

Command	**lacp port-priority** *port-priority*
Parameter Description	*port-priority*: Indicates the priority of an LACP member port. The value ranges from 0 to 65535.
Defaults	By default, the priority of an LACP member port is 32768.
Command Mode	Interface configuration mode of the specified physical port

Usage Guide	Use this command in global configuration mode to configure the priority of an LACP member port. To restore the settings, run **no lacp port-priority** in interface configuration mode.

Configuring the Timeout Mode of LACP Member Ports

- Optional.
- When you need to implement real-time link failure detection, configure the short timeout mode. It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.
- Perform this configuration on LACP-enabled devices, such as switches.

Command	**lacp short-timeout**
Parameter Description	N/A
Defaults	By default, the timeout mode of LACP member ports is long timeout.
Command Mode	Interface configuration mode
Usage Guide	The timeout mode is supported only by physical ports. To restore the default settings, run **no lacp short-timeout** in interface configuration mode.

Verification

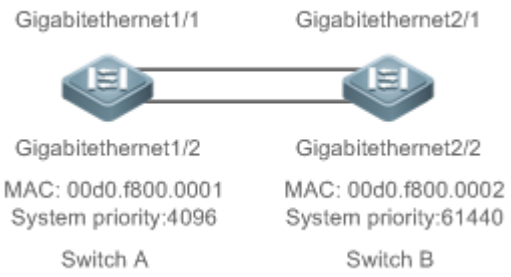
- Run **show running** to display the configuration.
- Run **show lacp summary** to display LACP link state.

Command	**show lacp summary** [*key-number*]
Parameter Description	*key-name*: Indicates the number of an LACP AP port.
Command Mode	Any mode
Usage Guide	The information on all LACP AP ports is displayed if you do not specify *key-name*.
	Ruijie(config)# show lacp summary 3 System Id:32768, 00d0.f8fb.0002 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State ---

	Gi0/1 SA bndl 4096 0x3 0x1 0x3d Gi0/2 SA bndl 4096 0x3 0x2 0x3d Gi0/3 SA bndl 4096 0x3 0x3 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi0/1 SA 61440 00d0.f800.0001 0x3 0x1 0x3d Gi0/2 SA 61440 00d0.f800.0001 0x3 0x2 0x3d Gi0/3 SA 61440 00d0.f800.0001 0x3 0x3 0x3d

Configuration Example

Configuring LACP

Scenario **Figure 3-2**	
Configuration Steps	● On Switch A, set the LACP system priority to 4096. ● Enable dynamic link aggregation on the GigabitEthernet1/1 and GigabitEthernet1/2 ports on Switch A and add the ports to LACP AP port 3. ● On Switch B, set the LACP system priority to 61440. ● Enable dynamic link aggregation on the GigabitEthernet2/1 and GigabitEthernet2/2 ports on Switch B and add the ports to LACP AP port 3.
Switch A	SwitchA# configure terminal SwitchA(config)# lacp system-priority 4096 SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# end
Switch B	SwitchB# configure terminal SwitchB(config)# lacp system-priority 61440

	SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# end
Verification	● Run **show lacp summary 3** to check whether LACP AP port 3 contains member ports GigabitEthernet2/1 and GigabitEthernet2/2.
Switch A	SwitchA# show LACP summary 3 System Id:32768, 00d0.f8fb.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi1/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d Gi1/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d
Switch B	SwitchB# show LACP summary 3 System Id:32768, 00d0.f8fb.0002 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port

```
Port        Flags       State       Priority            Key       Number      State
---------------------------------------------------------------------------
Gi2/1       SA          bndl        32768               0x3       0x1         0x3d
Gi2/2       SA          bndl        32768               0x3       0x2         0x3d
Partner information:
                        LACP port                       Oper      Port        Port
Port        Flags       Priority    Dev ID              Key       Number      State
---------------------------------------------------------------------------
Gi2/1       SA          32768       00d0.f800.0001      0x3       0x1         0x3d
Gi2/2       SA          32768       00d0.f800.0001      0x3       0x2         0x3d
```

3.4.3 Enabling LinkTrap

Configuration Effect

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

Configuration Steps

Enabling LinkTrap for an AP Port

- Optional.
- Enable LinkTrap in interface configuration mode. By default, LinkTrap is enabled. LinkTrap messages are sent when the link state or protocol state of the AP port is changed.
- Perform this configuration on AP-enabled devices.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, LinkTrap is enabled.
Command Mode	Interface configuration mode of the specified AP port
Usage Guide	Use this command in interface configuration mode to enable LinkTrap for the specified AP port. After LinkTrap is enabled, LinkTrap messages are sent when the link state of the AP port is changed. Otherwise, LinkTrap messages are not sent. By default, LinkTrap is enabled. To disable LinkTrap for an AP port, run **no snmp trap link-status** in interface configuration mode. LinkTrap cannot be enabled for a specific AP member port. To enable LinkTrap for all AP member ports, run **aggregateport member linktrap** in global configuration mode.

Enabling LinkTrap for AP Member Ports

- Optional.
- By default, LinkTrap is disabled for AP member ports.
- Perform this configuration on AP-enabled devices.

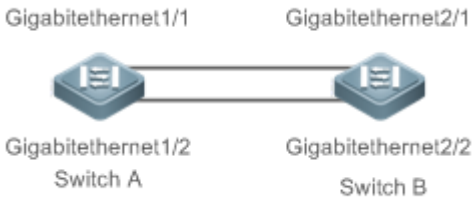
Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for AP member ports.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all AP member ports. By default, LinkTrap messages are not sent when the link state of AP member ports is changed. To disable LinkTrap for all AP member ports, run **no aggregateport member linktrap** in global configuration mode.

Verification

- Run **show running** to display the configuration.
- After LinkTrap is enabled, you can monitor this feature on AP ports or their member ports by using the MIB software.

Configuration Example

Enabling LinkTrap for AP Member Ports

Scenario **Figure 3-3**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, disable LinkTrap for AP port 3 and enable LinkTrap for its member ports. ● On Switch B, disable LinkTrap for AP port 3 and enable LinkTrap its AP member ports.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport member linktrap SwitchA(config)# interface Aggregateport 3 SwitchA(config-if-AggregatePort 3)# no snmp trap link-status
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport member linktrap SwitchB(config)# interface Aggregateport 3 SwitchB(config-if-AggregatePort 3)# no snmp trap link-status
Verification	● Run **show running** to check whether LinkTrap is enabled for AP port 3 and its member ports.
Switch A	SwitchA# show run | include AggregatePort 3

	Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchA# show run | include AggregatePort aggregateport member linktrap
Switch B	SwitchB# show run | include AggregatePort 3 Building configuration... Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchB# show run | include AggregatePort aggregateport member linktrap

3.4.4 Configuring a Load Balancing Mode

Configuration Effect

The system distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links. A device enabled with enhanced load balancing first determines the type of packets to be transmitted and performs load balancing based on the specified fields in the packets. For example, the AP port performs source IP-based load balancing on the packets containing an ever-changing source IPv4 address.

Notes

N/A

Configuration Steps

↘ **Configuring the Global Load Balancing Algorithm of an AP port**

- (Optional) Perform this configuration when you need to optimize load balancing.
- Perform this configuration on AP-enabled devices.

Command	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **src- l4port** | **dst-l4port** | **src-dst-l4port** | **src-ip-src-l4port** | **src-ip-dst-l4port** | **dst-ip-src-l4port** | **dst-ip-dst-l4port** | **src-ip-src-dst-l4port** | **dst-ip-src-dst-l4port** | **src-dst-ip-src-l4port** | **src-dst-ip-dst-l4port** }
Parameter	**dst-mac**: Indicates that load is distributed based on the destination MAC addresses of incoming packets.

Description	**src-mac**: Indicates that load is distributed based on the source MAC addresses of incoming packets. **src-dst-ip**: Indicates that load is distributed based on source and destination IP addresses of incoming packets. **dst-ip**: Indicates that load is distributed based on the destination IP addresses of incoming packets. **src-ip**: Indicates that load is distributed based on the source IP addresses of incoming packets. **src-dst-mac**: Indicates that load is distributed based on source and destination MAC addresses of incoming packets. **src-dst-ip-l4port**: Indicates that load is distributed based on source IP and destination IP addresses as well as Layer-4 source and destination port numbers. **src- l4port**: Indicates that load is distributed based on Layer-4 source port numbers. **dst- l4port**: Indicates that load is distributed based on Layer-4 destination port numbers. **src-dst-l4port**: Indicates that load is distributed based on Layer-4 source and destination port numbers. **src-ip-src-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 source port numbers. **src-ip-dst-l4port**: Indicates that load is distributed based on source IP addresses and Layer-4 destination port numbers. **dst-ip-src-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 source port numbers. **dst-ip-dst-l4port**: Indicates that load is distributed based on destination IP addresses and Layer-4 destination port numbers. **src-ip-src-dst-l4port:** Indicates that load is distributed based on source IP addresses as well as Layer-4 source and destination port numbers. **dst-ip-src-dst-l4port**: Indicates that load is distributed based on destination IP addresses as well as Layer-4 source and destination port numbers. **src-dst-ip-src-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 source port numbers. **src-dst-ip-dst-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer-4 destination port numbers.
Defaults	Load balancing can be based on source and destination MAC addresses (applicable to switches) or source and destination IP addresses (applicable to gateways).
Command Mode	Global configuration mode
Usage Guide	To restore the default settings, run **no aggregateport load-balance** in global configuration mode. You can run **aggregateport load-balance** in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run **no aggregateport load-balance** in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.

Verification

- Run **show running** to display the configuration.

- Run **show aggregateport load-balance** to display the load balancing configuration. If a device supports load balancing configuration on a specific AP port, run **show aggregateport summary** to display the configuration.
- Run **show load-balance-profile** to display the enhanced load balancing profile.

Command	**show aggregateport** *aggregate-port-number* [**load-balance | summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an AP port. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	The information on All AP ports is displayed if you do not specify the AP port number.
	Ruijie# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Configuration Example

Configuring a Load Balancing Mode

Scenario **Figure 3-4**	
Configuration Steps	● Add the GigabitEthernet 1/1 and GigabitEthernet 1/2 ports on Switch A to static AP port 3. ● Add the GigabitEthernet 2/1 and GigabitEthernet 2/2 ports on Switch B to static AP port 3. ● On Switch A, configure source MAC address-based load balancing for AP port 3 in global configuration mode. ● On Switch B, configure destination MAC address-based load balancing for AP port 3 in global configuration mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac

Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Verification	● Run **show aggregateport load-balance** to check the load balancing algorithm configuration.
Switch A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Switch B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

Common Errors

N/A

3.4.5 Configuring Aggregated Port Configuration Delivery from the AC

Configuration Effect

- After the AC delivers the aggregated port configuration to the AP, the corresponding wired port on the AP will be added to or exit from the corresponding aggregated port.

Notes

- To ensure normal link aggregation, static AP member ports need to be configured consistently on the two devices over a link.
- After an AP member port is added to an aggregated port, the member port cannot be added to other aggregated ports. The member port can be added to another aggregated port only after it exits from the original AP port.

Configuration Steps

↘ **Configuring Aggregated Port Configuration Delivery from the AC**

- Optional
- Perform this operation when a wired port of a specific AP, AP group, or all APs needs to be added to the AP aggregation group.

Command	**ap-interface wireport** *port-number* **port-group** *ap-number*
Parameter Description	**port-number**: Indicates the ID of the wired port on the AP. **ap-number**: Indicates the ID of the AP port.
Defaults	By default, the AC does not deliver aggregation port configuration.

Command Mode	ap-configure and ap-group configuration mode
Usage Guide	In ap-config and ap-group configuration mode, run **ap-interface wireport** *port-number* **port-group** *ap-number* to deliver an aggregated port configuration to enable a wired port on the AP to be added to the AP aggregation group, and run **no ap-interface wireport** *port-number* **port-group** for a specific wired port to exit from the AP aggregation group.

Verification

- Run **show running** to query the corresponding configuration.
- Run **show aggregateport summery** to query the corresponding relationship between the aggregated port and AP member ports.

Command	**show aggregateport summery**
Parameter Description	**ap-num**: Indicates the AP number.
Command Mode	All modes
Usage Guide	-
Command Presentation	Ruijie# show aggregateport summary AggregatePort MaxPorts Ports ---------- -------- ---------- Ag1 8 Gi0/1,Gi0/2

3.5 Monitoring

Displaying

Description	Command
Displays the summary or load balancing algorithm of an AP port.	**show aggregateport** [*ap-number*] { **load-balance** | **summary** }

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs an AP port.	**debug lsm ap**

4 Configuring VLAN

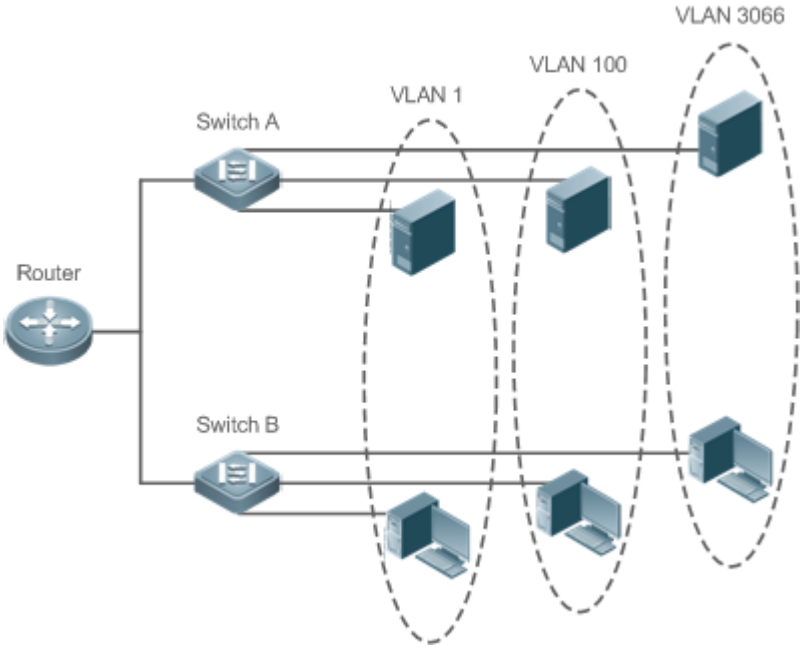
4.1 Overview

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer-2 networks of the OSI model.

A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

We may define a port as a member of a VLAN, and all terminals connected to this port are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing and modifying users. Communication among VLANs is realized through Layer-3 devices, as shown in the following figure.

Figure 4-1



Protocols and Standards

- IEEE 802.1Q

4.2 Applications

N/A

4.3 Features

Basic Concepts

VLAN

A VLAN is a logical network created based on a physical network. A VLAN has the same properties as a common LAN, except for physical location limitation. Unicast, broadcast and multicast frames of Layer 2 are forwarded and transmitted within a VLAN, keeping traffic segregated.

- The VLANs supported by Ruijie products comply with the IEEE802.1Q standard. A maximum of 4094 VLANs (VLAN ID 1-4094) are supported, among which VLAN 1 cannot be deleted.
- The configurable VLAN IDs are from 1 to 4094.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.

Port Mode

You can determine the frames allowed to pass a port and the VLANs which the port belongs to by configuring the port mode. See the following table for details.

Port Mode	Description
Access port	An Access port belongs to only one VLAN, which is specified manually.
Trunk port (802.1Q)	A Trunk port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs or the frames of allowed-VLANs.
Uplink port	An Uplink port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and tag the native VLAN egress traffic.
Hybrid port	A Hybrid port belongs to all the VLANs of an access switch by default, and it can forward the frames of all the VLANs and send frames of VLANs untagged. It can also transmit frames of allowed-VLANs.

Overview

Feature	Description
VLAN	VLAN helps realize Layer-2 isolation.

4.3.1 VLAN

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Working Principle

Every VLAN has an independent broadcast domain, and different VLANs are isolated on Layer 2.

Layer-2 isolation: If no SVIs are configured for VLANs, VLANs are isolated on Layer 2. This means users in these VLANs cannot communicate with each other.

Layer-3 interconnection: If SVIs are configured on a Layer-3 switch for VLANs, these VLANs can communicate with each other on Layer 3.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic VLAN	(Mandatory) It is used to create a VLAN.	
	vlan	Enters a VLAN ID.
	(Optional) It is used to configure an Access port to transmit the flows from a single VLAN.	
	switchport mode access	Defines a port as a Layer-2 Access port.
	switchport access vlan	Assigns a port to a VLAN.
	add interface	Adds one Access port or a group of such ports to the current VLAN.
	(Optional) It is used to rename a VLAN.	
	name	Names a VLAN.
Configuring a Trunk Port	(Mandatory) It is used to configure the port as a Trunk port.	
	switchport mode trunk	Defines a port as a Layer-2 Trunk port.
	(Optional) It is used to configure Trunk ports to transmit flows from multiple VLANs.	
	switchport trunk allowed vlan	Configures allowed-VLANs for a Trunk port.
	switchport trunk native vlan	Specifies a native VLAN for a Trunk port.
Configuring an Uplink Port	(Mandatory) It is used to configure the port as an Uplink port.	
	switchport mode uplink	Configures a port as an Uplink port.
	(Optional) It is used to restore the port mode.	
	no switchport mode	Restores the port mode.
Configuring a Hybrid Port	(Mandatory) It is used to configure a port as a Hybrid port.	
	switchport mode hybrid	Configures a port as a Hybrid port.
	(Optional) It is used to transmit the frames of multiple VLANs untagged.	
	no switchport mode	Restores the port mode.
	switchport hybrid allowed vlan	Configures allowed-VLANs for a Hybrid port.
	switchport hybrid native vlan	Configures a default VLAN for a Hybrid port.

4.4.1 Configuring Basic VLAN

Configuration Effect

- A VLAN is identified by a VLAN ID. You may add, delete, modify VLANs 2 to 4094, but VLAN 1 is created automatically and cannot be deleted. You may configure the port mode, and add or remove a VLAN.

Notes

- N/A

Configuration Steps

↘ Creating and Modifying a VLAN

- Mandatory.
- In case of insufficient hardware resources, the system returns information on VLAN creation failure.
- Use the vlan vlan-id command to create a VLAN or enter VLAN mode.

Command	**vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates VLAN ID ranging from 1 to 4094.
Defaults	VLAN 1 is created automatically and is not deletable.
Command Mode	Global configuration mode
Usage Guide	If you enter a new VLAN ID, the corresponding VLAN will be created. If you enter an existing VLAN ID, the corresponding VLAN will be modified. You may use the **no vlan** *vlan-id* command to delete a VLAN. The undeletable VLANs include VLAN1, the VLANs configured with SVIs, and SubVLANs.

↘ Renaming a VLAN

- Optional.
- You cannot rename a VLAN the same as the default name of another VLAN.
- Configuration:

Command	**name** *vlan-name*
Parameter Description	*vlan-name*: indicates a VLAN name.
Defaults	By default, the name of a VLAN is its VLAN ID. For example, the default name of the VLAN 4 is VLAN 0004.
Command Mode	VLAN configuration mode
Usage Guide	To restore the VLAN name to defaults, use the **no name** command.

↘ Assigning Current Access port to a Specified VLAN

- Optional.

- Use the **switchport mode access** command to specify Layer-2 ports (switch ports) as Access ports.
- Use the **switchport access vlan** *vlan-id* command to add an Access port to a specific VLAN so that the flows from the VLAN can be transmitted through the port.

Command	**switchport mode access**
Parameter Description	N/A
Defaults	A switch port is an Access port by default.
Command Mode	Interface configuration mode
Usage Guide	N/A

Command	**switchport access vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	An Access port is added to VLAN 1 by default.
Command Mode	Interface configuration mode
Usage Guide	If a port is assigned to a non-existent VLAN, the VLAN will be created automatically.

Adding an Access Port to Current VLAN

- Optional.
- This command takes effect only on an Access port. After an Access port is added to a VLAN, the flows of the VLAN can be transmitted through the port.

Command	**add interface** { *interface-id* | **range** *interface-range* }
Parameter Description	*interface-id*: indicates a single port. *interface-id*: indicates multiple ports.
Defaults	By default, all Layer-2 Ethernet ports belong to VLAN 1.
Command Mode	VLAN configuration mode
Usage Guide	In VLAN configuration mode, add a specific Access port to a VLAN. This command takes the same effect as command **switchport access vlan** *vlan-id*.

For the two commands of adding a port to a VLAN, the command configured later will overwrite the other one.

Verification

- Send untagged packets to an Access port, and they are broadcast within the VLAN.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	`Ruijie(config-vlan)#show vlan id 20` `VLAN Name Status Ports` `---- -------------------------------- --------- -----------------------------------` `20 VLAN0020 STATIC Gi0/1`

Configuration Example

Configuring Basic VLAN and Access Port

Configuration Steps	• Create a VLAN and rename it. • Add an Access port to the VLAN. There are two approaches. One is:
	`Ruijie# configure terminal` `Ruijie(config)# vlan 888` `Ruijie(config-vlan)# name test888` `Ruijie(config-vlan)# configure terminal` `Ruijie(config)# interface GigabitEthernet 0/3` `Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access`

	Ruijie(config-if-GigabitEthernet 0/3)# switchport access vlan 20 The other approach is adding an Access port (GigabitEthernet 0/3) to VLAN20: Ruijie# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface GigabitEthernet 0/3
Verification	Check whether the configuration is correct.
	Ruijie(config-vlan)#show vlan VLAN Name Status Ports ---- -------------------------------- --------- ---------------------------------- 1 VLAN0001 STATIC **20 VLAN0020 STATIC Gi0/3** **888 test888 STATIC** Ruijie(config-vlan)# Ruijie# show interface GigabitEthernet 0/3 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- --------- ------ ------ --------- -------------- GigabitEthernet 0/3 **enabled ACCESS 20 1 Disabled ALL**

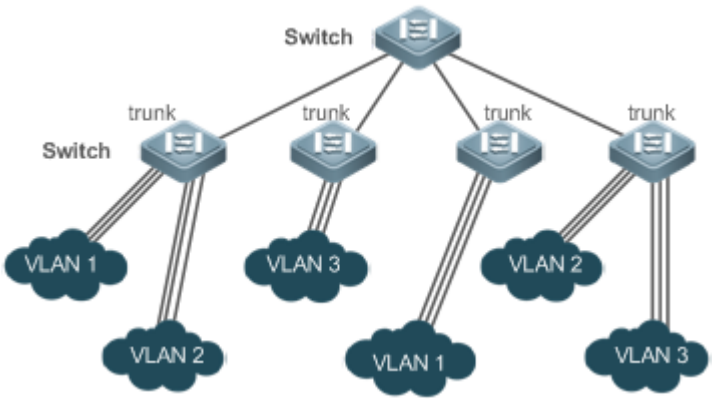
4.4.2 Configuring a Trunk Port

Configuration Effect

A Trunk is a point-to-point link connecting one Ethernet interface or multiple ones to other network devices (for example, a router or switch) and it may transmit the flows from multiple VLANs.

The Trunk of Ruije devices adopts the 802.1Q encapsulation standard. The following figure displays a network adopting a Trunk connection.

Figure 4-2



You may configure an Ethernet port or Aggregate Port (See *Configuring Aggregate Port* for details) as a Trunk port.

You should specify a native VLAN for a Trunk port. The untagged packets received by and sent from the Trunk port are considered to belong to the native VLAN. The default VLAN ID (PVID in the IEEE 802.1Q) of this Trunk port is the native VLAN ID. Meanwhile, frames of the native VLAN sent via the Trunk are untagged. The default native VLAN of a Trunk port is VLAN 1.

When configuring a Trunk link, make sure the Trunk ports at the two ends of the link adopt the same native VLAN.

Configuration Steps

Configuring a Trunk Port

- Mandatory.
- Configure a Trunk port to transmit the flows from multiple VLANs.

Command	**switchport mode trunk**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Trunk.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a Trunk port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.
- By default, a trunk port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Trunk port.

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	The parameter vlan-list can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs. **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Defaults	The Trunk port and the Uplink port belong to all VLANs.
Command Mode	Interface configuration mode
Usage Guide	To restore the configuration on a Trunk port to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- A Trunk port receives and sends tagged or untagged 802.1Q frames. Untagged frames transmit the flows from the native VLAN. The default native VLAN is VLAN 1.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Trunk port.

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default VALN for a Trunk/Uplink port is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of a Trunk port back to defaults, use the **no switchport trunk native vlan** command.

When you set the native VLAN of a port to a non-existent VLAN, this VLAN will not be created automatically. Besides, the native VLAN can be out of the list of allowed-VLANs for this port. In this case, the flows from the native VLAN cannot pass through the port.

Verification

- Send tag packets to a Trunk port, and they are broadcast within the specified VLANs.

- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Ruijie(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

- N/A

Common Errors

- N/A

4.4.3 Configuring an Uplink Port

Configuration Effect

- An Uplink port is usually used in QinQ (the IEEE 802.1ad standard) environment, and is similar to a Trunk port. Their difference is that an Uplink port only transmits tagged frames while a Trunk port sends untagged frames of the native VLAN.

Configuration Steps

Configuring an Uplink Port

- Mandatory.
- Configure an Uplink port to transmit the flows from multiple VLANS, but only tagged frames can be transmitted.

Command	**switchport mode uplink**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Uplink.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of an Uplink port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Trunk Port

- Optional.

- You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through an Uplink port.

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	The parameter *vlan-list* can be a VLAN or some VLANs, and the VLAN IDs are connected by "-" in order. For example: 10–20. **all** indicates allowed-VLANs include all VLANs; **add** indicates adding a specific VLAN to the list of allowed-VLANs; **remove** indicates removing a specific VLAN from the list of allowed-VLANs; **except** indicates adding all VLANs except those in the listed VLAN to the list of allowed-VLANs; and **only** indicates adding the listed VLANs to the list of allowed-VLANs, and removing the other VLANs from the list.
Command Mode	Interface configuration mode
Usage Guide	To restore the allowed-VLANs to defaults (**all**), use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will not be stripped when it passes an Uplink port. This is contrary to a Trunk port.

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of an Uplink to defaults, use the **no switchport trunk native vlan** command.

Verification

- Send tag packets to an Uplink port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Ruijie(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring an Uplink Port

Configuration Steps	The following is an example of configuring Gi0/1 as an Uplink port.
	Ruijie# configure terminal Ruijie(config)# interface gi 0/1 Ruijie(config-if-GigabitEthernet 0/1)# switchport mode uplink Ruijie(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	Ruijie# show interfaces GigabitEthernet 0/1 switchport Interface Switchport Mode Access Native Protected VLAN lists GigabitEthernet 0/1 enabled UPLINK 1 1 disabled ALL

4.4.4 Configuring a Hybrid Port

Configuration Effect

- A Hybrid port is usually used in SHARE VLAN environment. By default, a Hybrid port is the same as a Trunk port. Their difference is that a Hybrid port can send the frames from the VLANs except the default VLAN in the untagged format.

Configuration Steps

Configuring a Hybrid Port

- Mandatory.
- Configure a Hybrid port to transmit the flows from multiple VLANs.

Command	**switchport mode hybrid**
Parameter Description	N/A
Defaults	The default mode is Access, which can be modified to Hybrid.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a Hybrid port to defaults, use the **no switchport mode** command.

Defining Allowed-VLANs for a Hybrid Port

- Optional.
- By default, a Hybrid port transmits the flows from all the VLANs (1 to 4094). You may configure a list of allowed-VLANs to prohibit flows of some VLANs from passing through a Hybrid port.

Command	**switchport hybrid allowed vlan** [[**add** | **only**] **tagged** | [**add**] **untaged** | **remove**] *vlan_list*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	By default a Hybrid port belongs to all VLANs. The port is added to the default VLAN in untagged form and to the other VLANs in the tagged form.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a Hybrid port.

Command	**switchport hybrid native vlan** *vlan_id*
Parameter Description	*vlan-id*: indicates a VLAN ID.
Defaults	The default native VLAN is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the native VLAN of a Hybrid port to defaults, use the **no switchport hybrid native vlan** command.

Verification

- Send tagged packets to an Hybrid port, and they are broadcast within the specified VLANs.
- Use commands **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id* **:** indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A
Command Display	Ruijie(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ----------------------------------- **20 VLAN0020 STATIC Gi0/1**

Configuration Example

Configuring a Hybrid Port

Configuration Steps	The following is an example of configuring Gi0/1 as a Hybrid port.

	Ruijie# configure terminal Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3 Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30 Ruijie(config-if-GigabitEthernet 0/1)# end
Verification	Check whether the configuration is correct.
	Ruijie(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration... Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode **hybrid** switchport hybrid **native vlan 3** switchport hybrid allowed vlan add **untagged 20-30**

4.5 Monitoring

Displaying

Description	Command
Displays VLAN configuration.	**show vlan**
Displays configuration of switch ports.	**show interface switchport**

Debugging

⚠ System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs VLANs.	**debug bridge vlan**

5 Configuring Super VLAN

5.1 Overview

Super virtual local area network (VLAN) is an approach to dividing VLANs.Super VLAN is also called VLAN aggregation, and is a management technology tailored for IP address optimization.

Using super VLAN can greatly save IP addresses. Only one IP address needs to be assigned to the super VLAN that consists of multiple sub VLANs, which greatly saves IP addresses and facilitates network management.

5.2 Application

Application	Description
Sharing One IP Gateway Among Multiple VLANs	VLANs are divided to implement layer-2 (L2) isolation of access users. All VLAN users share one IP gateway to implement layer-3 (L3) communication and communication with external networks.

5.2.1 Sharing One IP Gateway Among Multiple VLANs

Scenario

Multiple VLANs are isolated at L2 on a L3 device, but users of these VLANs can perform L3 communication with each other in the same network segment.

Deployment

On the intranet, use the super VLAN so that multiple sub VLANs can share one IP gateway and meanwhile VLANs are mutually isolated at L2.

Users in sub VLANs can perform L3 communication through the gateway of the super VLAN.

5.3 Features

Basic Concepts

↘ Super VLAN

Super VLAN is also called VLAN aggregation, and is a management technology tailored for IP address optimization. It aggregates multiple VLANs to one IP network segment. No physical port can be added to a super VLAN. The switch virtual interface (SVI) is used to manage the cross-VLAN communication of sub VLANs. The super VLAN cannot be used as a common 802.1Q VLAN, but can be treated as the primary VLAN of sub VLANs.

Sub VLAN

A sub VLAN is an independent broadcast domain. Sub VLANs are mutually isolated at L2. Users of sub VLANs of the same or different super VLANs communicate with each other through the L3 SVIs of their own super VLANs.

ARP Proxy

A L3 SVI can be created only for a super VLAN. Users in a sub VLAN communicates with users in other sub VLANs of the same super VLAN or users in other network segments through the ARP proxy and the L3 SVI of the super VLAN. When a user of a sub VLAN sends an ARP request to a user of another sub VLAN, the gateway of the super VLAN uses its own MAC addressto send or respond to the ARP requests. The process is called ARP proxy.

IP Address Range of the Sub VLAN

Based on the gateway IP address configured for the super VLAN, an IP address range can be configured for each sub VLAN.

Overview

Feature	Description
Super VLAN	Create a L3 interface as anSVI to allow all sub VLANs to share the same IP network segment through the ARP proxy.

5.3.1 Super VLAN

Users of all sub VLANs of a super VLAN can be allocated IP addresses in the same IP address range, and share the same IP gateway. Users can implement cross-VLAN communication through this gateway. It is unnecessary to allocate a gateway for every VLAN, which saves the IP addresses.

Working Principle

IP addresses in a network segment are allocated to different sub VLANs that belong to the same super VLAN. Each sub VLAN has an independent broadcast domain of the VLAN, and different sub VLANs are isolated from each other at L2. When users in sub VLANs need to perform L3 communication, the IP address of the SVI of the super VLAN is used as the gateway address. In this way, multiple VLANs share the same IP gateway, and it is unnecessary to configure a gateway for every VLAN. In addition, to implement L3 communication between sub VLANs and between sub VLANs and other network segments, the ARP proxy function is used to forward and process the ARP requests and responses.

L2 communication of sub VLANs: If the SVI is not configured for the super VLAN, sub VLANs of super VLAN are mutually isolated at L2, that is, users in different sub VLANs cannot communicate with each other. If the SVI is configured for the super VLAN, and the gateway of the super VLAN can function as the ARP proxy, users in different sub VLANs of the same super VLAN can communicate with each other. This is because IP addresses of users in different sub VLANs belong to the same network segment, and communication between these users is still treated as L2 communication.

L3 communication of sub VLANs: If users in sub VLANs of a super VLAN need to perform L3 communication across network segments, the gateway of this super VLAN functions as the ARP proxy to respond to the ARP requests in place of sub VLANs.

5.4 Configuration

Configuration Item	Description and Command	
Configuring Basic Functions of the Super VLAN	Mandatory.	
	supervlan	Configures a super VLAN.
	subvlan*vlan-id-list*	Configures a sub VLAN.
	proxy-arp	Enables the ARP proxy function.
	interface vlan*vlan-id*	Creates a virtual interface for a super VLAN.
	ip address*ip mask*	Configures the IP address of the virtual interface of a super VLAN.
	Optional.	
	subvlan-address-range *start-ip end-ip*	Specifies the IP address range in a sub VLAN.

5.4.1 Configuring Basic Functions of the Super VLAN

Configuration Effect

Enable the super VLAN function and configure an SVI for the super VLAN to implement L2/L3 communication between sub VLANs across VLANs.

Users in all sub VLANs of a super VLAN share the same IP gateway. It is unnecessary to specify a network segment for every VLAN, which saves the IP addresses.

Notes

- A super VLAN does not belong to any physical port. Therefore, the device configured with the super VLAN cannot process packets that contain the super VLAN tag.
- Both the super VLAN function and the ARP proxy function of each sub VLAN must be enabled.
- An SVI and an IP address must be configured for a super VLAN. The SVI is a virtual interface used for communication of users in all sub VLANs.

Configuration Steps

Configuring a Super VLAN

- Mandatory.
- No physical port exists in a super VLAN.
- The ARP proxy function must be enabled. This function is enabled by default.

A super VLAN is valid only after you configure sub VLANs for this super VLAN.

VLAN 1 cannot be configured as a super VLAN.

A super VLAN cannot be configured as a sub VLAN of another super VLAN. A sub VLAN of a super VLAN cannot be configured as a super VLAN.

Command	**supervlan**
Parameter Description	N/A
Defaults	N/A
Command Mode	VLAN configuration mode
Usage Guide	By default, the super VLAN function is disabled. No physical port can be added to a super VLAN. Once a VLAN is not a super VLAN, all its sub VLANs become common static VLANs.

Configuring a Virtual Interface for a Super VLAN

- Mandatory.
- No physical port can be added to a super VLAN. You can configure the L3 SVI for a VLAN.

When a super VLAN is configure with an SVI, it allocates a L3 interface i to each sub VLANs. If a sub VLAN is not allocated a L3 interfacedue to resource deficiency, the sub VLAN becomes a common VLAN again.

Command	**interface vlan***vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of the super VLAN.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A L3 interface must be configured as the virtual interface of a super VLAN.

Configuring the Gateway of a Super VLAN

- Mandatory.
- The IP gateway on the L3 SVI is configured as the proxy for all users in sub VLANs to respond to ARP requests.

Command	**ip address***ip mask*
Parameter Description	*ip*: Indicates the IP address of the gateway on the virtual interface of a super VLAN. *Mask*: Indicates the mask.
Defaults	N/A
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the gateway for a super VLAN. Users of all sub VLANs of the super VLAN

	share this gateway.

Configuring a Sub VLAN

- Mandatory.
- Physical ports can be added to sub VLANs. Sub VLANs of a super VLAN share the gateway address of the super VLAN and reside in the same network segment.
- The ARP proxy function must be enabled. This function is enabled by default.

You must change a sub VLAN into a common VLAN before you can delete this sub VLAN by running the **no vlan** command.

One sub VLAN belongs to only one super VLAN.

Command	**subvlan***vlan-id-list*
Parameter Description	*vlan-id-list* : Specifies multiple VLANs as sub VLANs of a super VLAN.
Defaults	N/A
Command Mode	VLAN configuration mode
Usage Guide	Connection interfaces can be added to a sub VLAN. You must change a sub VLAN into a common VLAN before you can delete this sub VLAN by running the **no vlan** [*id*]command. You cannot configure a L3 SVI of the VLAN for a sub VLAN. If you have configured a L3 SVI for a super VLAN, the attempt of adding more sub VLANs may fail due to resource deficiency. If you configure sub VLANs to a super VLAN, and then configure a L3 SVI of the VLAN for a super VLAN, some sub VLANs may become common VLANs again due to resource deficiency.

Configuring the ARP Proxy

- (Mandatory) The ARP proxy function is enabled by default.
- Users in sub VLANs can implement L2/L3 communication across VLANs through the gateway proxy only after the ARP proxy function is enabled on both the super VLAN and sub VLANs.

The ARP proxy function must be enabled on both the super VLAN and sub VLANs.Otherwise, this function does not take effect.

Command	**proxy-arp**
Parameter Description	N/A
Defaults	N/A
Command Mode	VLAN configuration mode

Usage Guide	By default, the ARP proxy function is enabled. Run this command to enable the ARP proxy function on both the super VLAN and sub VLANs. Users in sub VLANs can implement L2/L3 communication across VLANs only after the ARP proxy function is enabled on both the super VLAN and sub VLANs.

Configuring the IP Address Range of the Sub VLAN

- You can allocate an IP address range to each sub VLAN. Users in a sub VLAN can communicate with users of other VLANs only when their IP addresses are in the specified range.
- Unless otherwise specified, you do not need to configure the IP address range.

IP addresses dynamically allocated to users through DHCP may not be in the allocated IP address range. If the IP addresses allocated through DCHP are not in the specified range, users in a sub VLAN cannot communicate with users of other VLANs. Therefore, be cautious in using the **subvlan-address-range** *start-ip end-ip*command.

The IP address range of a sub VLAN must be within the IP address range of the super VLAN to which the sub VLAN belongs.Otherwise, users in sub VLANs cannot communicate with each other.

IP addresses of users in a sub VLAN must be within the IP address range of the sub VLAN.Otherwise, users in the sub VLAN cannot communicate with each other.

Command	**subvlan-address-range** *start-ip end-ip*
Parameter Description	*start-ip*: Indicates the start IP address of a sub VLAN. *end-ip*: Indicates the end IP address of a sub VLAN.
Defaults	N/A
Command Mode	VLAN configuration mode
Usage Guide	Optional. Run this command to configure the IP address range of users in a sub VLAN. IP address ranges of different sub VLANs of a super VLAN cannot overlap with each other. The IP address range of a sub VLAN must be within the IP address range of the super VLAN to which the sub VLAN belongs. Otherwise, users in sub VLANs cannot communicate with each other. Users in a sub VLAN can communicate with users of other VLANs only when their IP addresses (either dynamically allocated through DHCP or statically configured) are in the configured IP address range. IP addresses allocated through DHCP may not be in the configured IP address range. In this case, users in a sub VLAN cannot communicate with users of other VLANs. Therefore, be cautious when using this command.

Verification

After each sub VLAN is correlated with the gateway of the super VLAN, users in sub VLANs can ping each other.

Configuration Example

- N/A

Common Errors

The SVI and IP gateway are not configured for the super VLAN. Consequently, communication fails between sub VLANs and between sub VLANs and other VLANs.

The ARP proxy function is disabled on the super VLAN or sub VLANs. Consequently, users in sub VLANs cannot communicate with users of other VLANs.

The IP address range of the sub VLAN is configured, but IP addresses allocated to users are not in this range.

5.5 Monitoring

Displaying

Description	Command
Displays the super VLAN configuration.	**show supervlan**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the super VLAN.	**debug bridge svlan**

6 Configuring MSTP

6.1 Overview

Spanning Tree Protocol (STP) is a Layer-2 management protocol. It cannot only selectively block redundant links to eliminate Layer-2 loops but also can back up links.

Similar to many protocols, STP is continuously updated from Rapid Spanning Tree Protocol (RSTP) to Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer-2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes two times of the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP: Since all VLANs in a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be balanced among VLANs.

MSTP, defined by the IEEE in 802.1s, resolves defects of STP and RSTP. It cannot only rapidly converge but also can enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

In general, STP/RSTP works based on ports while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

Ruijie devices support STP, RSTP, and MSTP, and comply with IEEE 802.1D, IEEE 802.1w, and IEEE 802.1s.

Protocols and Standards

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w: Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

6.2 Applications

Application	Description
MSTP+VRRP Dual-Core Topology	With a hierarchical network architecture model, the MSTP+VRRP mode is used to implement redundancy and load balancing to improve system availability of the network.

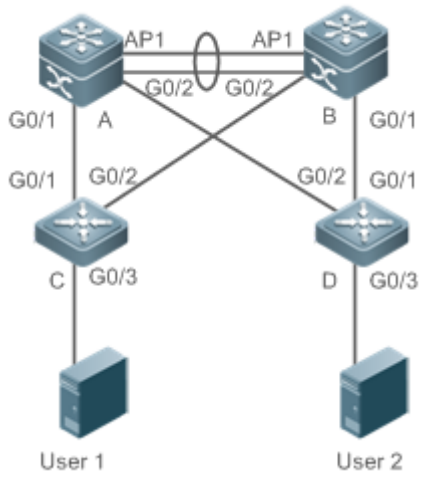
6.2.1 MSTP+VRRP Dual-Core Topology

Scenario

The typical application of MSTP is the MSTP+VRRP dual-core solution. This solution is an excellent solution to improve system availability of the network. Using a hierarchical network architecture model, it is generally divided into three layers (core layer, convergence layer, and access layer) or two layers (core layer and access layer). They form the core network system to provide data exchange service.

The main advantage of this architecture is its hierarchical structure. In the hierarchical network architecture, all capacity indicators, characteristics, and functions of network devices at each layer are optimized based on their network locations and roles, enhancing their stability and availability.

Figure 6-1 MSTP+VRRP Dual-Core Topology



Remarks	The topology is divided into two layers: core layer (Devices A and B) and access layer (Devices C and D).

Deployment

- Core layer: Multiple MSTP instances are configured to realize load balancing. For example, two instances are created: Instance 1 and Instance 2. Instance 1 maps VLAN 10 while Instance 2 maps VLAN 20. Device A is the root bridge of Instances 0 and 1 (Instance 0 is CIST, which exists by default). Device B is the root bridge of Instance 2.
- Core layer: Devices A and B are the active VRRP devices respectively on VLAN 10 and VLAN 20.
- Access layer: Configure the port directly connected to the terminal (PC or server) as a PortFast port, and enable BPDU guard to prevent unauthorized users from accessing illegal devices.

6.3 Features

Basic Concepts

BPDU

To generate a stable tree topology network, the following conditions must be met:

- Each bridge has a unique ID consisting of the bridge priority and MAC address.
- The overhead of the path from the bridge to the root bridge is called root path cost.
- A port ID consists of the port priority and port number.

Bridges exchange BPDU packets to obtain information required for establishing the best tree topology. These packets use the multicast address 01-80-C2-00-00-00 (hexadecimal) as the destination address.

A BPDU consists of the following elements:

- Root bridge ID assumed by the local bridge
- Root path cost of the local bridge
- Bridge ID (ID of the local bridge)
- Message age (age of a packet)
- Port ID (ID of the port sending this packet)
- **Forward-Delay Time**, **Hello Time**, **Max-Age Time** are time parameters specified in the MSTP.
- Other flags, such as flags indicating network topology changes and local port status.

If a bridge receives a BPDU with a higher priority (smaller bridge ID and lower root path cost) at a port, it saves the BPDU information at this port and transmits the information to all other ports. If the bridge receives a BPDU with a lower priority, it discards the information.

Such a mechanism allows information with higher priorities to be transmitted across the entire network. BPDU exchange results are as follows:

- A bridge is selected as the root bridge.
- Except the root bridge, each bridge has a root port, that is, a port providing the shortest path to the root bridge.
- Each bridge calculates the shortest path to the root bridge.

- Each LAN has a designated bridge located in the shortest path between the LAN and the root bridge. A port designated to connect the bridge and the LAN is called designated port.
- The root port and designated port enter the forwarding status.

Bridge ID

According to IEEE 802.1W, each bridge has a unique ID. The spanning tree algorithm selects the root bridge based on the bridge ID. The bridge ID consists of eight bytes, of which the last six bytes are the MAC address of the bridge. In its first two bytes (as listed in the following table), the first four bits indicate the priority; the last eight bits indicate the system ID for use in extended protocol. In RSTP, the system ID is 0. Therefore, the bridge priority should be a integral multiple of 4,096.

	Bit	Value
Priority value	16	32,768
	15	16,384
	14	8,192
	13	4,096
System ID	12	2,048
	11	1,024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

Spanning-Tree Timers

The following three timers affect the performance of the entire spanning tree:

- Hello timer: Interval for periodically sending a BPDU packet.
- Forward-Delay timer: Interval for changing the port status, that is, interval for a port to change from the listening state to the learning state or from the learning state to the forwarding state when RSTP runs in STP-compatible mode.
- Max-Age timer: The longest time-to-live (TTL) of a BPDU packet. When this timer elapses, the packet is discarded.

Port Roles and Port States

Each port plays a role on a network to reflect different functions in the network topology.

- Root port: Port providing the shortest path to the root bridge.
- Designated port: Port used by each LAN to connect the root bridge.

- Alternate port: Alternative port of the root port. Once the root port loses effect, the alternate port immediately changes to the root port.
- Backup port: Backup port of the designated port. When a bridge has two ports connected to a LAN, the port with the higher priority is the designated port while the port with the lower priority is the backup port.
- Disabled port: Inactive port. All ports with the operation state being down play this role.

The following figures show the roles of different ports:

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise specified, port priorities decrease from left to right.

Figure 6-2

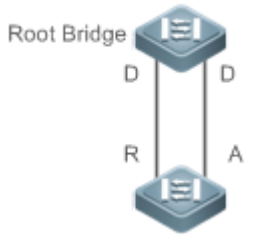


Figure 6-3

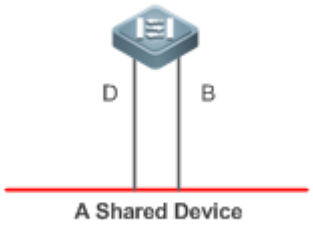
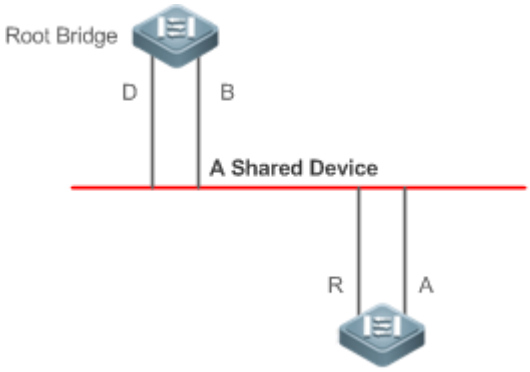


Figure 6-4



Each port has three states indicating whether to forward data packets so as to control the entire spanning tree topology.

- Discarding: Neither forwards received packets nor learns the source MAC address.
- Learning: Does not forward received packets but learns the source MAC address, which is a transitive state.

- Forwarding: Forwards received packets and learns the source MAC address.

For a stable network topology, only the root port and designated port can enter the forwarding state while other ports are always in discarding state.

Hop Count

Internal spanning trees (ISTs) and multiple spanning tree instances (MSTIs) calculate whether the BPDU packet time expires based on an IP TTL-alike mechanism Hop Count, instead of Message Age and Max Age.

It is recommended to run the **spanning-tree max-hops** command in global configuration mode to configure the hop count. In a region, every time a BPDU packet passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU packet time expires and the device discards the packet.

To be compatible with STP and RSTP outside the region, MSTP also retains the Message Age and Max Age mechanisms.

Overview

Feature	Description
STP	STP, defined by the IEEE in 802.1D, is used to eliminate physical loops at the data link layer in a LAN.
RSTP	RSTP, defined by the IEEE in 802.1w, is optimized based on STP to rapidly converge the network topology.
MSTP	MSTP, defined by the IEEE in 802.1s, resolves defects of STP, RSTP, and Per-VLAN Spanning Tree (PVST). It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.
MSTP Optical Features	MSTP includes the following features: PortFast, BPDU guard, BPDU filter, TC protection, TC guard, TC filter, BPDU check based on the source MAC address, BPDU filter based on the illegal length, Auto Edge, root guard, and loop guard.

6.3.1 STP

STP is used to prevent broadcast storms incurred by loops and provide link redundancy.

Working Principle

For the Layer-2 Ethernet, only one active link can exist between two LANs. Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

6.3.2 RSTP

RSTP is completely compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

Working Principle

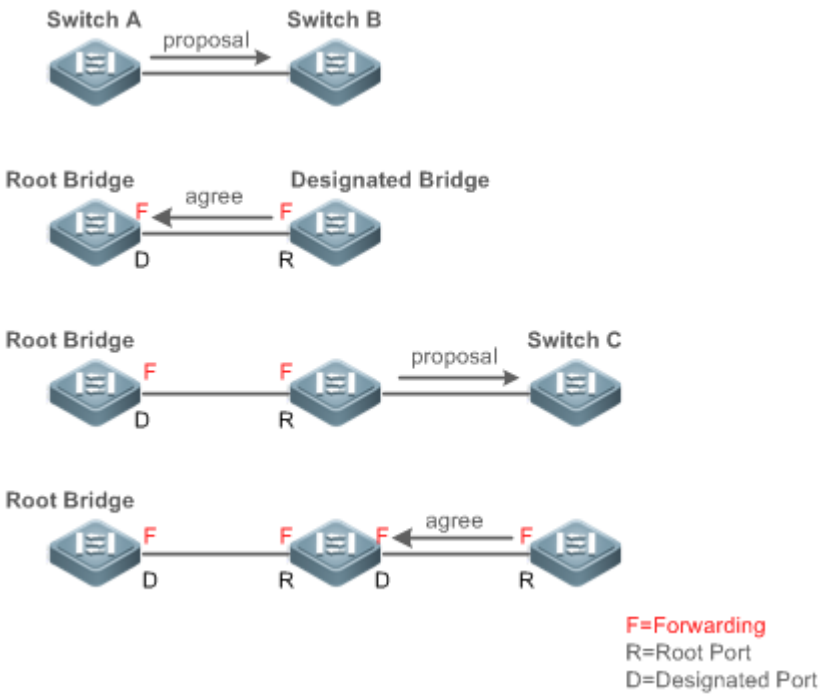
Fast RSTP Convergence

RSTP has a special feature, that is, to make ports quickly enter the forwarding state.

STP enables a port to enter the forwarding state 30 seconds (two times of the Forward-Delay Time; the Forward-Delay Time can be configured, with a default value of 15 seconds) after selecting a port role. Every time the topology changes, the root port and designated port reselected by each bridge enter the forwarding state 30 seconds later. Therefore, it takes about 50 seconds for the entire network topology to become a tree.

RSTP differs greatly from STP in the forwarding process. As shown in Figure 6-, Switch A sends an RSTP Proposal packet to Switch B. If Switch B finds the priority of Switch A higher, it selects Switch A as the root bridge and the port receiving the packet as the root port, enters the forwarding state, and then sends an Agree packet from the root port to Switch A. If the designated port of Switch A is agreed, the port enters the forwarding state. Switch B's designated port resends a Proposal packet to extend the spanning tree by sequence. Theoretically, RSTP can recover the network tree topology to rapidly converge once the network topology changes.

Figure 6-5



The above handshake process is implemented only when the connection between ports is in point-to-point mode. To give the devices their full play, it is recommended not to enable point-to-point connection between devices.

Figure 6- and Figure 6- show the examples of non point-to-point connection.

Example of non point-to-point connection:

Figure 6-6

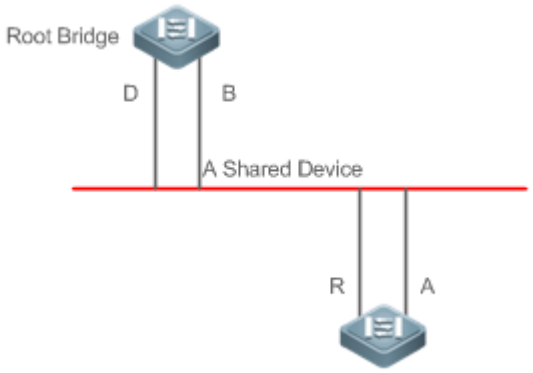


Figure 6-7

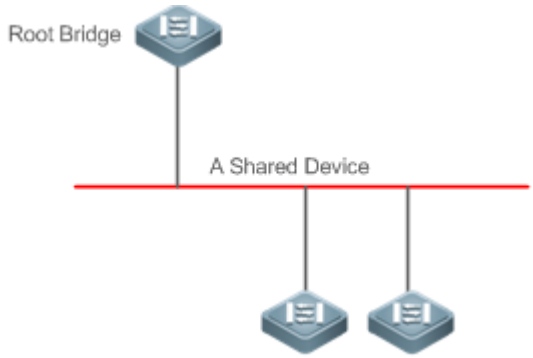
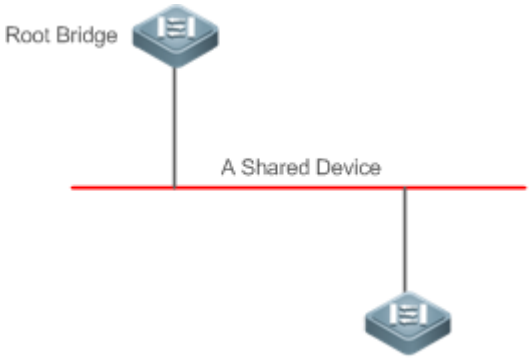


Figure 6- shows an example of point-to-point connection.

Figure 6-8



Compatibility Between RSTP and STP

RSTP is completely compatible with STP. RSTP automatically checks whether the connected bridge supports STP or RSTP based on the received BPDU version number. If the port connects to an STP bridge, the port enters the forwarding state 30 seconds later, which cannot give RSTP its full play.

Another problem may occur when RSTP and STP are used together. As shown in the following figures, Switch A (RSTP) connects to Switch B (STP). If Switch A finds itself connected to an STP bridge, it sends an STP BPDU packet. However, if Switch B is replaced with Switch C (RSTP) but Switch A still sends STP BPDU packets, Switch C will assume itself connected to the STP bridge. As a result, two RSTP devices work under STP, greatly reducing the efficiency.

RSTP provides the protocol migration feature to forcibly send RSTP BPDU packets (the peer bridge must support RSTP). In this case, Switch A is enforced to send an RSTP BPDU and Switch C then finds itself connected to the RSTP bridge. As a result, two RSTP devices work under RSTP, as shown in Figure 6-.

Figure 6-9

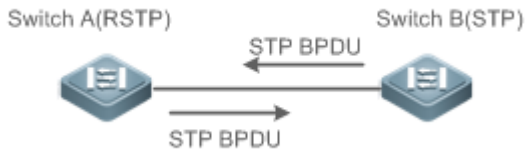


Figure 6-10

6.3.3 MSTP

MSTP resolves defects of STP and RSTP. It cannot only rapidly converge but also can forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

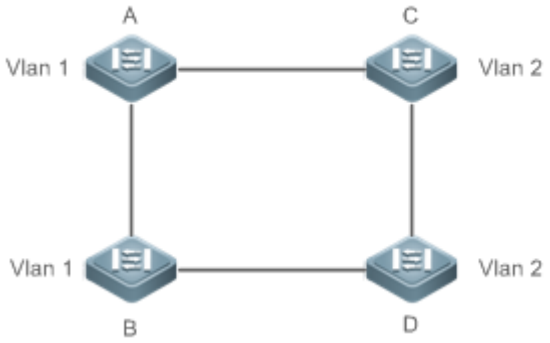
Working Principle

Ruijie devices support MSTP. MSTP is a new spanning tree protocol developed from traditional STP and RSTP and includes the fast RSTP forwarding mechanism.

Since traditional spanning tree protocols are irrelevant to VLANs, problems may occur in specific network topologies:

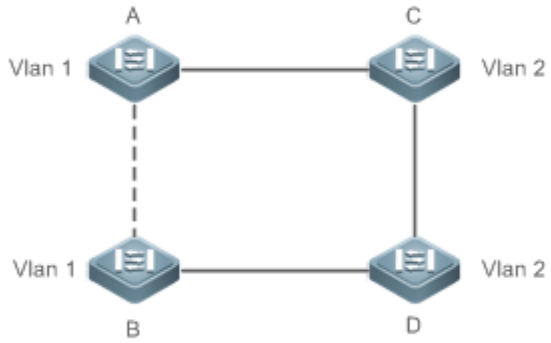
As shown in Figure 6-, Devices A and B are in VLAN 1 while Devices C and D are in VLAN 2, forming a loop.

Figure 6-11



If the link from Device A to Device B through Devices C and D costs less than the link from Device A direct to Device B, the link between Device A and Device B enters the discarding state (as shown in Figure 6-). Since Devices C and D do not include VLAN 1 and cannot forward data packets of VLAN 1, VLAN 1 of Device A fails to communicate with VLAN 1 of Device B.

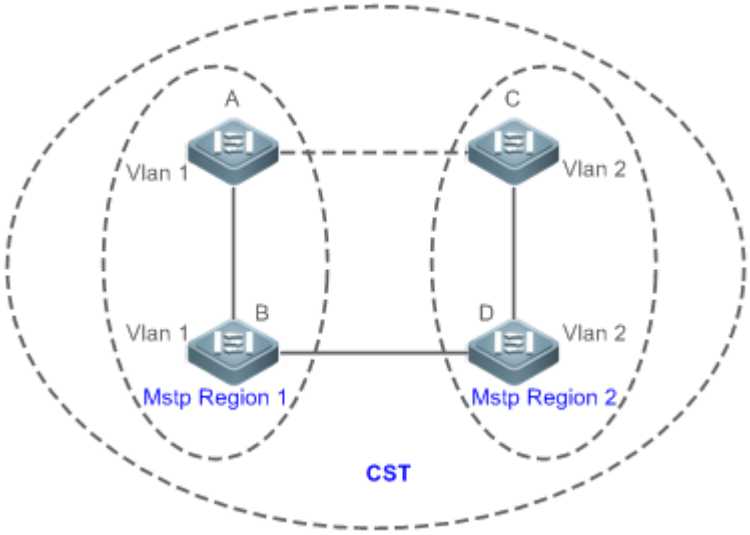
Figure 6-12



MSTP is developed to resolve this problem. It divides one or multiple VLANs of a device into an instance. Devices configured with the same instance form an MST region to run an independent spanning tree (called IST). This MST region, like a big device, implements the spanning tree algorithm with other MST regions to generate a complete spanning tree called common spanning tree (CST).

Based on this algorithm, the above network can form the topology shown in Figure 6- under the MSTP algorithm: Devices A and B are in MSTP region 1 in which no loop occurs, and therefore no link enters the discarding state. This also applies to MSTP Region 2. Region 1 and Region 2, like two big devices having loops, select a link to enter the discarding state based on related configuration.

Figure 6-13



This prevents loops to ensure proper communication between devices in the same VLAN.

MSTP Region Division

To give MSTP its due play, properly divide MSTP regions and configure the same MST configuration information for devices in the same MSTP region.

MST configuration information include:

- MST configuration name: Consists of at most 32 bytes to identify an MSTP region.
- MST Revision Number: Consists of 16 bits to identify an MSTP region.
- MST instance-VLAN mapping table: A maximum number of 64 instances (with their IDs ranging from 1 to 64) are created for each device and Instance 0 exists mandatorily. Therefore, the system supports a maximum number of 65 instances. Users can assign 1 to 4,994 VLANs belonging to different instances (ranging from 0 to 64) as required. Unassigned VLANs belong to Instance 0 by default. In this case, each MSTI is a VLAN group and implements the spanning tree algorithm of the MSTI specified in the BPDU packet, not affected by CIST and other MSTIs.

Run the **spanning-tree mst configuration** command in global configuration mode to enter the MST configuration mode to configure the above information.

MSTP BPDUs carry the above information. If the BPDU received by a device carries the same MST configuration information with the information on the device, it regards that the connected device belongs to the same MST region with itself. Otherwise, it regards the connected device originated from another MST region.

It is recommended to configure the instance-VLAN mapping table after disabling MSTP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

IST (Spanning Tree in an MSTP Region)

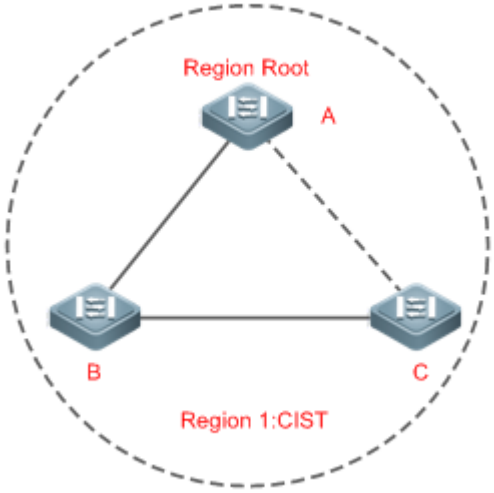
After MSTP regions are divided, each region selects an independent root bridge for each instance based on the corresponding parameters such as bridge priority and port priority, assigns roles to each port on each device, and specifies whether the port is in forwarding or discarding state in the instance based on the port role.

Through MSTP BPDU exchange, an IST is generated and each instance has their own spanning trees (MSTIs), in which the spanning tree corresponding to Instance 0 and CST are uniformly called Common Instance Spanning Tree (CIST). That is, each instance provides a single and loop-free network topology for their own VLAN groups.

As shown in Figure 6-, Devices A, B, and C form a loop in Region 1.

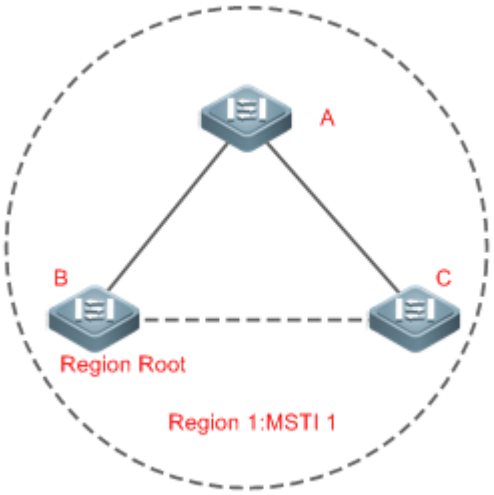
As shown in Figure 6-,, Device A has the highest priority in the CIST (Instance 0) and thereby is selected as the region root. Then MSTP enables the link between A and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 0, only links from A to B and from B to C are available, interrupting the loop of this VLAN group.

Figure 6-14



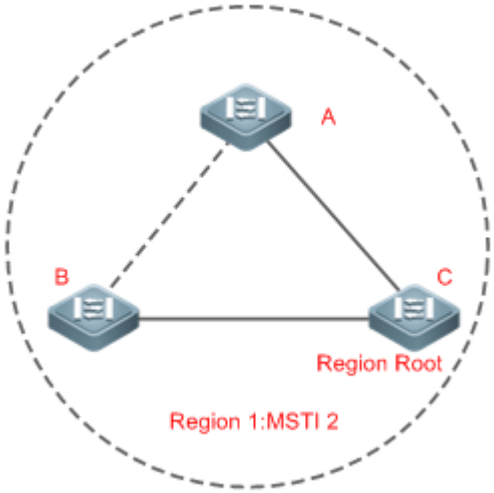
As shown in Figure 6-, Device B has the highest priority in the MSTI 1 (Instance 1) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 1, only links from A to B and from A to C are available, interrupting the loop of this VLAN group.

Figure 6-15



As shown in Figure 6-, Device C has the highest priority in the MSTI 2 (Instance 2) and thereby is selected as the region root. Then MSTP enables the link between B and C to enter the discarding state based on other parameters. Therefore, for the VLAN group of Instance 2, only links from B to C and from A to C are available, interrupting the loop of this VLAN group.

Figure 6-16

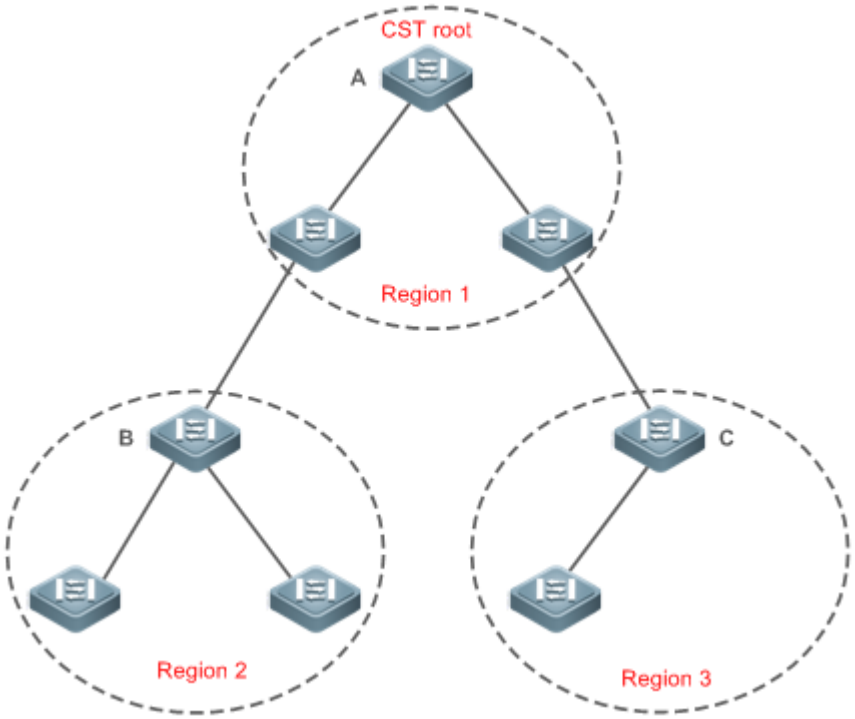


Note that MSTP does not care which VLAN a port belongs to. Therefore, users should configure the path cost and priority of a related port based on the actual VLAN configuration to prevent MSTP from interrupting wrong loops.

↘ CST (Spanning Tree Between MSTP Regions)

Each MSTP region is like a big device for the CST. Different MSTP regions form a bit network topology tree called CST. As shown in Figure 6-, Device A, of which the bridge ID is the smallest, is selected as the root in the entire CST and the CIST regional root in this region. In Region 2, since the root path cost from Device B to the CST root is lowest, Device B is selected as the CIST regional root in this region. For the same reason, Device C is selected as the CIST regional root.

Figure 6-17



The CIST regional root may not be the device of which the bridge ID is the smallest in the region but indicates the device of which the root path cost from this region to the CST root is the smallest.

For the MSTI, the root port of the CIST regional root has a new role "master port". The master port acts as the outbound port of all instances and is in forwarding state for all instances. To make the topology more stable, we suggest that the master port of each region to the CST root be on the same device of the region if possible.

Compatibility Among MSTP, RSTP, and STP

Similar to RSTP, MSTP sends STP BPDUs to be compatible with STP. For details, see "Compatibility Between RSTP and STP".

Since RSTP processes MSTP BPDUs of the CIST, MSTP does not need to send RSTP BPDUs to be compatible with it.

Each STP or RSTP device is a single region and does not form the same region with any devices.

6.3.4 MSTP Optional Features

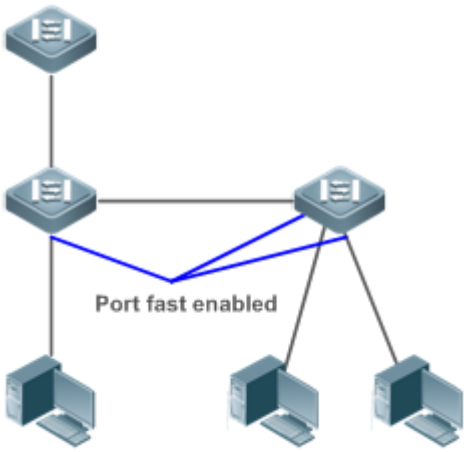
MSTP optional features mainly include PortFast port, BPDU guard, BPDU filter, TC guard, and guard. The optional features are mainly used to deploy MSTP configurations based on the network topology and application characteristics in the MSTP network. This enhances the stability, robustness, and anti-attack capability of MSTP, meeting application requirements of MSTP in different customer scenarios.

Working Principle

PortFast

If a port of a device connects directly to the network terminal, this port is configured as a PortFast port to directly enter the forwarding state. If the PortFast port is not configured, the port needs to wait for 30 seconds to enter the forwarding state. Figure 6- shows which ports of a device can be configured as PortFast ports.

Figure 6-18



If a PortFast port still receives BPDUs, its Port Fast Operational State is Disabled and the port enters the forwarding state according to the normal STP algorithm.

BPDU Guard

BPDU guard can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpduguard default** command in global configuration mode to enable global BPDU guard. If PortFast is enabled on a port or this port is automatically identified as an edge port, this port enters the error-disabled state to indicate the configuration error immediately after receiving a BPDU. At the same time, the port is disabled, indicating that a network device may be added by an unauthorized user to change the network topology.

It is also recommended to run the **spanning-tree bpduguard enable** command in interface configuration mode to enable BPDU guard on a port (whether PortFast is enabled or not on the port). In this case, the port enters the error-disabled state immediately after receiving a BPDU.

BPDU Filter

BPDU filter can be enabled globally or enabled on an interface.

It is recommended to run the **spanning-tree portfast bpdufilter default** command in global configuration mode to enable global BPDU filter. In this case, the PortFast port neither receives nor sends BPDUs and therefore the host connecting directly to the PortFast port receives no BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically loses effect.

It is also recommended to run the **spanning-tree bpdufilter enable** command in interface configuration mode to enable BPDU filter on a port (whether PortFast is enabled or not on the port). In this case, the port neither receives nor sends BPDUs but directly enters the forwarding state.

TC Protection

TC BPDUs are BPDU packets carrying the TC. If a switch receives such packets, it indicates the network topology changes and the switch will delete the MAC address table. For Layer-3 switches in this case, the forwarding module is re-enabled and the port status in the ARP entry changes. When a switch is attacked by forged TC BPDUs, it will frequently perform the above operations, causing heavy load and affecting network stability. To prevent this problem, you can enable TC protection.

TC protection can only be globally enabled or disabled. This function is disabled by default.

When TC protection is enabled, the switch deletes TC BPDUs within a specified period (generally 4 seconds) after receiving them and monitors whether any TC BPDU packet is received during the period. If a device receives TC BPDU packets during this period, it deletes them when the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries.

TC Guard

TC protection ensures less dynamic MAC addresses and ARP entries removed when a large number of TC packets are generated on the network. However, a device receiving TC attack packets still performs many removal operations and TC packets can be spread, affecting the entire network. Users can enable TC guard to prevent TC packets from spreading globally or on a port. If TC guard is enabled globally or on a port, a port receiving TC packets filters these TC packets or TC packets generated by itself so that TC packets will not be spread to other ports. This can effectively control possible TC attacks in the network to ensure network stability. Particularly on Layer-3 devices, this function can effectively prevent the access-layer device from flapping and interrupting the core route.

- If TC guard is used incorrectly, the communication between networks is interrupted.
- It is recommended to enable this function only when illegal TC attack packets are received in the network.
- If TC guard is enabled globally, no port spreads TC packets to others. This function can be enabled only on laptop access devices.
- If TC guard is enabled on a port, the topology changes incurred and TC packets received on the port will not be spread to other ports. This function can be enabled only on uplink ports, particularly on ports of the convergence core.

TC Filter

If TC guard is enabled on a port, the port does not forward TC packets received and generated by the port to other ports performing spanning tree calculation on the device. When the status of a port changes (for example, from blocking to forwarding), the port generates TC packets, indicating that the topology may have changed.

In this case, since TC guard prevents TC packets from spreading, the device may not clear the MAC addresses of the port when the network topology changes, causing a data forwarding error.

To resolve this problem, TC filter is introduced. TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes. If TC filter is enabled, the address removal problem will be avoided and the core route will not be interrupted when ports not enabled with PortFast frequently go up or down, and the core routing entries can be updated in a timely manner when the topology changes.

- TC filter is disabled by default.

BPDU Source MAC Address Check

BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address. If you run the **no bpdu src-mac-check** command to disable BPDU source MAC address check on a port, the port receives all BPDU packets.

BPDU Filter

If the Ethernet length of a BPDU exceeds 1,500, this BPDU will be discarded, preventing receipt of illegal BPDU packets.

Auto Edge

If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.

You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

This function is enabled by default.

- If Auto Edge conflicts with the manually configured PortFast, the manual configuration prevails.
- Since this function is used for rapid negotiation and forwarding between the designated port and the downlink port, STP does not support this function. If the designated port is in forwarding state, the Auto Edge configuration does not take effect on this port. It takes only when rapid negotiation is re-performed, for example, when the network cable is removed and plugged.
- If BPDU filter has been enabled on a port, the port directly enters the forwarding state and is not automatically identified as an edge port.
- This function applies only to the designated port.

Root Guard

In the network design, the root bridge and backup root bridge are usually divided into the same region. Due to incorrect configuration of maintenance personnel or malicious attacks in the network, the root bridge may receive configuration information with a higher priority and thereby switches to the backup root bridge, causing incorrect changes in the network topology. Root guard is to resolve this problem.

If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.

If a port enters the blocking state due to root guard, you can manually restore the port to the normal state by disabling root guard on this port or disabling spanning tree guard (running **spanning-tree guard none** in interface configuration mode).

- If root guard is used incorrectly, the network link will be interrupted.
- If root guard is enabled on a non-designated port, this port will be enforced as a designated port and enter the BKN state. This indicates that the port enters the blocking state due to root inconsistency.

If a port enters the BKN state due to receipt of configuration information with a higher priority in MST0, this port will be enforced in the BKN state in all other instances.

Root guard and loop guard cannot take effect on a port at the same time.

Loop Guard

Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

If a port enabled with loop guard does not receive BPDUs, the port switches its role but stays in discarding state till it receives BPDUs and recalculates the spanning tree.

You can enable loop guard globally or on a port.

Root guard and loop guard cannot take effect on a port at the same time.

Before MSTP is restarted on a port, the port enters the blocking state in loop guard. If the port still receives no BPDU after MSTP is restarted, the port will become a designated port and enter the forwarding state. Therefore, it is recommended to identify the cause why a port enters the blocking state in loop protection and rectify the fault as soon as possible before restarting MSTP. Otherwise, the spanning tree topology will still become abnormal after MSTP is restarted.

BPDU Transparent Transmission

In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

BPDU transparent transmission is disabled by default.

BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

6.4 Configuration

Configuration	Description and Command	
Enabling STP	(Mandatory) It is used to enable STP.	
	spanning-tree	Enables STP and configures basic attributes.
	spanning-tree mode	Configures the STP mode.
Configuring STP Compatibility	(Optional) It is used to be compatible with competitor devices.	
	spanning-tree compatible enable	Enables the compatibility mode of a port.

Configuration	Description and Command	
	clear spanning-tree detected-protocols	Performs mandatory version check for BPDUs.
Configuring an MSTP Region	⚠ (Optional) It is used to configure an MSTP region.	
	spanning-tree mst configuration	Enters the MST configuration mode.
Enabling Fast RSTP Convergence	⚠ (Optional) It is used to configure whether the link type of a port is point-to-point connection.	
	spanning-tree link-type	Configures the link type.
Configuring Priorities	⚠ (Optional) It is used to configure the switch priority or port priority.	
	spanning-tree priority	Configures the switch priority.
	spanning-tree port-priority	Configures the port priority.
Configuring the Port Path Cost	⚠ (Optional) It is used to configure the path cost of a port or the default path cost calculation method.	
	spanning-tree cost	Configures the port path cost.
	spanning-tree pathcost method	Configures the default path cost calculation method.
Configuring the Maximum Hop Count of a BPDU Packet	⚠ (Optional) It is used to configure the maximum hop count of a BPDU packet.	
	spanning-tree max-hops	Configures the maximum hop count of a BPDU packet.
Enabling PortFast-related Features	⚠ (Optional) It is used to enable PortFast-related features.	
	spanning-tree portfast	Enables PortFast.
	spanning-tree portfast bpduguard default	Enables BPDU guard on all ports.
	spanning-tree bpduguard enabled	Enables BPDU guard on a port.
	spanning-tree portfast bpdufilter default	Enables BPDU filter on all ports.
	spanning-tree bpdufilter enabled	Enables BPDU filter on a port.
Enabling TC-related Features	⚠ (Optional) It is used to enable TC-related features.	
	spanning-tree tc-protection	Enables TC protection.
	spanning-tree tc-protection tc-guard	Enables TC guard on all ports.
	spanning-tree tc-guard	Enables TC guard on a port.
	spanning-tree ignore tc	Enables TC filter on a port.
Enabling BPDU Source MAC Address Check	⚠ (Optional) It is used to enable BPDU source MAC address check.	
	bpdu src-mac-check	Enables BPDU source MAC address check on a port.

Configuration	Description and Command	
Configuring Auto Edge	(Optional) It is used to configure Auto Edge.	
	spanning-tree autoedge	Enables Auto Edge on a port. This function is enabled by default.
Enabling Guard-related Features	(Optional) It is used to enable port guard features.	
	spanning-tree guard root	Enables root guard on a port.
	spanning-tree loopguard default	Enables loop guard on all ports.
	spanning-tree guard loop	Enables loop guard on a port.
	spanning-tree guard none	Disables the guard feature on a port.
Enabling BPDU Transparent Transmission	(Optional) It is used to enable BPDU transparent transmission	
	bridge-frame forwarding protocol bpdu	Enables BPDU transparent transmission.

6.4.1 Enabling STP

Configuration Effect

- Enable STP globally and configure the basic attributes.
- Configure the STP mode.

Notes

- STP is disabled by default. Once STP is enabled, the device starts to run STP. The device runs MSTP by default.
- The default STP mode is MSTP mode.
- STP and Transparent Interconnection of Lots of Links (TRILL) of the data center cannot be enabled at the same time.

Configuration Steps

Enabling STP

- Mandatory.
- Unless otherwise specified, enable STP on each device.
- Run the spanning-tree [forward-time seconds | hello-time seconds | max-age seconds] command to enable STP and configure basic attributes.
- The forward-time ranges from 4 to 30. The hello-time ranges from 1 to 10. The max-age ranges from 6 to 40.
- Running the clear commands may lose vital information and thus interrupt services. The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time –1 second). Otherwise, the topology may become unstable.

Command	**spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **tx-hold-count** *numbers*]

Parameter Description	**forward-time** *seconds*: Indicates the interval when the port status changes. The value ranges from 4 to 30 seconds. The default value is 15 seconds. **hello-time** *seconds*: Indicates the interval when a device sends a BPDU packet. The value ranges from 1 to 10 seconds. The default value is 2 seconds. **max-age** *second*: Indicates the longest TTL of a BPDU packet. The value ranges from 6 to 40 seconds. The default value is 20 seconds. **tx-hold-count** *numbers*: Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.
Defaults	STP is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The value ranges of forward-time, hello-time, and max-age are related. If one of them is modified, the other two ranges are affected. The three values must meet the following condition: 2 x (Hello Time + 1 second) <= Max-Age Time <= 2 x (Forward-Delay Time – 1 second) Otherwise, the topology may become unstable.

Configuring the STP Mode

- Optional.
- According to related 802.1 protocol standards, STP, RSTP, and MSTP are mutually compatible, without any configuration by the administrator. However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. Therefore, Ruijie provides a command for the administrator to switch the STP mode to a lower version if other vendors' devices are incompatible with Ruijie devices.
- Run the **spanning-tree mode** [**stp | rstp | mstp**] command to modify the STP mode.

Command	**spanning-tree mode** [**stp** | **rstp** | **mstp**]
Parameter Description	**stp**: Spanning Tree Protocol (IEEE 802.1d) **rstp**: Rapid Spanning Tree Protocol (IEEE 802.1w) **mstp**: Multiple Spanning Tree Protocol (IEEE 802.1s)
Defaults	The default value is **mstp**.
Command Mode	Global configuration mode
Usage Guide	However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the STP mode to a lower version.

Verification

- Display the configuration.

Configuration Example

Enabling STP and Configuring Timer Parameters

Scenario **Figure 6-19**	
Configuration Steps	● Enable STP and set the STP mode to STP on the devices. ● Configure the timer parameters of root bridge DEV A as follows: Hello Time=4s, Max Age=25s, Forward Delay=18s.
DEV A	Step 1: Enable STP and set the STP mode to STP. `Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#spanning-tree` `Ruijie(config)#spanning-tree mode stp` Step 2: Configure the timer parameters of root bridge DEV A. `Ruijie(config)#spanning-tree hello-time 4` `Ruijie(config)#spanning-tree max-age 25` `Ruijie(config)#spanning-tree forward-time 18`
DEV B	Enable STP and set the STP mode to STP. `Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#spanning-tree` `Ruijie(config)#spanning-tree mode stp`
Verification	● Run the **show spanning-tree summary** command to display the spanning tree topology and protocol configuration parameters.
DEV A	`Ruijie#show spanning-tree summary` `Spanning tree enabled protocol stp` `  Root ID    Priority    0`

	Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 0 Address 00d0.f822.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	Ruijie#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 001a.a917.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Bound(STP) Gi0/1 Root FWD 20000 128 False P2p Bound(STP)

Common Errors

The timer parameters will take effect only after the device has been elected as a root bridge.

6.4.2 Configuring STP Compatibility

Configuration Effect

- Enable the compatibility mode of a port to realize interconnection between Ruijie devices and other SPs' devices.
- Enable protocol migration to perform forcible version check to affect the compatibility between RSTP and STP.

Notes

- If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between Ruijie devices and other SPs' devices.

Configuration Steps

Enabling the Compatibility Mode on a Port

- Optional.

Command	**spanning-tree compatible enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between Ruijie devices and other SPs' devices.

Enabling Protocol Migration

- Optional.
- If the peer device supports RSTP, you can enforce version check on the local device to force the two devices to run RSTP.

Command	**clear spanning-tree detected-protocols** [**interface** *interface-id*]
Parameter Description	**interface** *interface-id*: Indicates a port.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to enforce a port to send RSTP BPDU packets and perform forcible check on them.

Verification

- Display the configuration.

Configuration Example

Enabling STP Compatibility

Scenario **Figure 6-20**	
Configuration Steps	● Configure Instances 1 and 2 on Devices A and B, and map Instance 1 with VLAN 10 and Instance 2 with VLAN 20. ● Configure Gi0/1 and Gi0/2 to respectively belong to VLAN 10 and VLAN 20, and enable STP compatibility.
DEV A	Step 1: Configure Instances 1 and 2, and map Instances 1 and 2 respectively with VLANs 10 and 20. `Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#spanning-tree mst configuration` `Ruijie(config-mst)#instance 1 vlan 10` `Ruijie(config-mst)#instance 2 vlan 20` Step 2: Configure the VLAN the port belongs to, and enable STP compatibility on the port. `Ruijie(config)#int gi 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 10` `Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable` `Ruijie(config-if-GigabitEthernet 0/1)#int gi 0/2` `Ruijie(config-if-GigabitEthernet 0/2)#switchport access vlan 20` `Ruijie(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable`
DEV B	Perform the same steps as DEV A.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated.
DEV A	`Ruijie#show spanning-tree summary` `Spanning tree enabled protocol mstp`

```
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    32768
             Address     001a.a917.78cc
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Desg FWD 20000      128      False    P2p
Gi0/1            Desg FWD 20000      128      False    P2p

MST 1 vlans map : 10
  Region Root Priority   32768
             Address     001a.a917.78cc
             this bridge is region root

  Bridge ID  Priority    32768
             Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Desg FWD 20000      128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   32768
             Address     001a.a917.78cc
             this bridge is region root
```

	Bridge ID Priority 32768 Address 001a.a917.78cc Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p
DEV B	Ruijie#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 001a.a917.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 00d0.f822.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Gi0/1 Root FWD 20000 128 False P2p MST 1 vlans map : 10 Region Root Priority 32768 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 00d0.f822.3344

```
Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Root FWD 20000      128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   32768
             Address     001a.a917.78cc
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Root FWD 20000      128      False    P2p
```

Common Errors

It is recommended to configure a same VLAN list on the two sides of the link.

6.4.3 Configuring an MSTP Region

Configuration Effect

- Configure an MSTP region to adjust which devices belong to the same MSTP region and thereby affect the network topology.

Notes

- To make multiple devices belong to the same MSTP region, configure the same name, revision number, and instance-VLAN mapping table for them.
- You can configure VLANs for Instances 0 to 64, and then the remaining VLANs are automatically allocated to Instance 0. One VLAN belongs to only one instance.
- It is recommended to configure the instance-VLAN mapping table after disabling STP. After the configuration, re-enable MSTP to ensure stability and convergence of the network topology.

Configuration Steps

Configuring an MSTP Region

- Optional.
- Configure an MSTP region when multiple devices need to belong to the same MSTP region.

Command	**spanning-tree mst configuration**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the MST configuration mode.

Configuring the Relationship between MST Instance and Vlan

Command	**instance** *instance-id* **vlan** *vlan-range*
Parameter Description	*instance-id*: Indicates the MSTI ID, ranging from 0 to 64. *vlan-range*: Indicates the VLAN ID, ranging from 1 to 4,094.
Command Mode	MST configuration mode
Usage Guide	To add a VLAN group to an MSTI, run this command. For example, instance 1 vlan 2-200: Adds VLANs 2 to 200 to Instance 1. instance 1 vlan 2,20,200: Adds VLANs 2, 20, and 200 to Instance 1. You can use the **no** form of this command to remove VLANs from an instance. Removed VLANs are automatically forwarded to Instance 0.

Configuring MST Name

Command	**name** *name*
Parameter Description	*name*: Indicates the MST name. It consists of a maximum of 32 bytes.
Command Mode	MST configuration mode
Usage Guide	N/A

Configuring MST Version

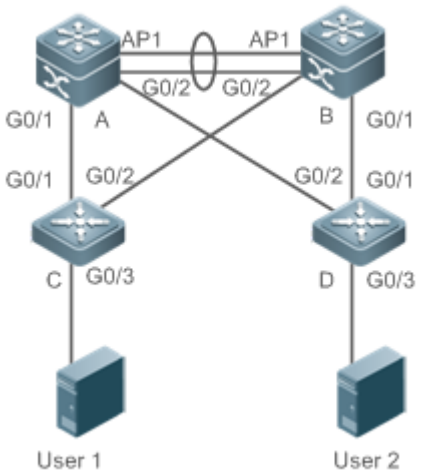
Command	**revision** *version*
Parameter Description	*version*: Indicates the MST revision number, ranging from 0 to 65,535.
Command Mode	MST configuration mode
Usage Guide	N/A

Verification

- Display the configuration.

Configuration Example

Enabling MSTP to Achieve VLAN Load Balancing in the MSTP+VRRP Topology

Scenario **Figure 6-21**	
Configuration Steps	• Enable MSTP and create Instances 1 and 2 on Switches A, B, C, and D. • Configure Switch A as the root bridge of Instances 0 and 1 and Switch B as the root bridge of Instance 2. • Configure Switch A as the VRRP master device of VLANs 1 and 10 and Switch B as the VRRP master device of VLAN 20.
A	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports. `A(config)#vlan 10` `A(config-vlan)#vlan 20` `A(config-vlan)#exit` `A(config)#int range gi 0/1-2` `A(config-if-range)#switchport mode trunk` `A(config-if-range)#int ag 1` `A(config-if-AggregatePort 1)# switchport mode trunk` Step 2: Enable MSTP and create Instances 1 and 2. `A(config)#spanning-tree` `A(config)# spanning-tree mst configuration` `A(config-mst)#instance 1 vlan 10`

```
A(config-mst)#instance 2 vlan 20
A(config-mst)#exit
```

Step 3: Configure Switch A as the root bridge of Instances 0 and 1.

```
A(config)#spanning-tree mst 0 priority 4096
A(config)#spanning-tree mst 1 priority 4096
A(config)#spanning-tree mst 2 priority 8192
```

Step 4: Configure VRRP priorities to enable Switch A to act as the VRRP master device of VLAN 10, and configure the virtual gateway IP address of VRRP.

```
A(config)#interface vlan 10
A(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0
A(config-if-VLAN 10) vrrp 1 priority 120
A(config-if-VLAN 10) vrrp 1 ip 192.168.10.1
```

Step 5 Set the VRRP priority to the default value 100 to enable Switch A to act as the VRRP backup device of VLAN 20.

```
A(config)#interface vlan 20
A(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0
A(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
```

B

Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports.

```
B(config)#vlan 10
B(config-vlan)#vlan 20
B(config-vlan)#exit
B(config)#int range gi 0/1-2
B(config-if-range)#switchport mode trunk
B(config-if-range)#int ag 1
B(config-if-AggregatePort 1)# switchport mode trunk
```

Step 2: Enable MSTP and create Instances 1 and 2.

```
B(config)#spanning-tree
B(config)# spanning-tree mst configuration
```

	B(config-mst)#instance 1 vlan 10 B(config-mst)#instance 2 vlan 20 B(config-mst)#exit Step 3: Configure Switch A as the root bridge of Instance 2. B(config)#spanning-tree mst 0 priority 8192 B(config)#spanning-tree mst 1 priority 8192 B(config)#spanning-tree mst 2 priority 4096 Step 4: Configure the virtual gateway IP address of VRRP. B(config)#interface vlan 10 B(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0 B(config-if-VLAN 10) vrrp 1 ip 192.168.10.1 Step 5 Set the VRRP priority to 120 to enable Switch B to act as the VRRP backup device of VLAN 20. B(config)#interface vlan 20 B(config-if-VLAN 20)vrrp 1 priority 120 B(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0 B(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
C	Step 1: Configure VLANs 10 and 20, and configure ports as Trunk ports. C(config)#vlan 10 C(config-vlan)#vlan 20 C(config-vlan)#exit C(config)#int range gi 0/1-2 C(config-if-range)#switchport mode trunk Step 2: Enable MSTP and create Instances 1 and 2. C(config)#spanning-tree C(config)# spanning-tree mst configuration C(config-mst)#instance 1 vlan 10 C(config-mst)#instance 2 vlan 20 C(config-mst)#exit

	Step 3: Configure the port connecting Device C directly to users as a PortFast port and enable BPDU guard. C(config)#int gi 0/3 C(config-if-GigabitEthernet 0/3)#spanning-tree portfast C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
D	Perform the same steps as Device C.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated. ● Run the **show vrrp brief** command to check whether the VRRP master/backup devices are successfully created.
A	Ruijie#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 4096 Address 00d0.f822.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 1 vlans map : 10 Region Root Priority 4096

```
            Address     00d0.f822.3344
            this bridge is region root

  Bridge ID  Priority    4096
            Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Desg FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   4096
            Address     001a.a917.78cc
            this bridge is region root

  Bridge ID  Priority    8192
            Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p
```

B

```
Ruijie#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
            Address     00d0.f822.3344
```

```
            this bridge is root
            Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    8192
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

MST 1 vlans map : 10
  Region Root Priority   4096
             Address     00d0.f822.3344
             this bridge is region root

  Bridge ID  Priority    8192
             Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

MST 2 vlans map : 20
  Region Root Priority   4096
             Address     001a.a917.78cc
             this bridge is region root
```

```
  Bridge ID  Priority    4096
             Address     001a.a917.78cc


Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Desg FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p
```

C

```
Ruijie#show spanning-tree summary


Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
             Address     00d0.f822.3344
             this bridge is root
             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    32768
             Address     001a.a979.00ea
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     Type  OperEdge
---------------- ---- --- ---------- -------- ----- ---------------
Fa0/2            Altn BLK 200000     128      P2p   False
Fa0/1            Root FWD 200000     128      P2p   False


MST 1 vlans map : 10
  Region Root Priority   4096
             Address     00d0.f822.3344
             this bridge is region root
```

	Bridge ID Priority 32768 Address 001a.a979.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 2 vlans map : 20 Region Root Priority 4096 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 001a.a979.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Root FWD 200000 128 P2p False Fa0/1 Altn BLK 200000 128 P2p False
D	Omitted.

Common Errors

- MST region configurations are inconsistent in the MSTP topology.
- VLANs are not created before you configure the mapping between the instance and VLAN.
- A device runs STP or RSTP in the MSTP+VRRP topology, but calculates the spanning tree according to the algorithms of different MST regions.

6.4.4 Enabling Fast RSTP Convergence

Configuration Effect

- Configure the link type to make RSTP rapidly converge.

Notes

- If the link type of a port is point-to-point connection, RSTP can rapidly converge. For details, see "Fast RSTP Convergence". If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port. If a port is in full duplex mode, the device sets the link type to point-to-point. If a port is in half duplex mode, the device sets the link type to shared. You can also forcibly configure the link type to determine whether the port connection is point-to-point connection.

Configuration Steps

Configuring the Link Type

- Optional.

Command	**spanning-tree link-type** [**point-to-point** | **shared**]
Parameter Description	**point-to-point**: Forcibly configures the link type of a port to be point-to-point. **shared**: Forcibly configures the link type of a port to be shared.
Command Mode	Interface configuration mode
Usage Guide	If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Enabling Fast RSTP Convergence

Configuration Steps	Set the link type of a port to point-to-point.
	`Ruijie(config)#int gi 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point`
Verification	- Run the **show spanning-tree summary** command to display the link type of the port.
	`Ruijie#show spanning-tree summary` `Spanning tree enabled protocol mstp` `MST 0 vlans map : ALL` `  Root ID    Priority    32768` `            Address     001a.a917.78cc`

```
            this bridge is root
            Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec


  Bridge ID  Priority    32768
             Address     00d0.f822.3344
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec


Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Root FWD 20000      128      False    P2p
```

Common Errors

If a port is in half duplex mode, the device sets the link type to shared.

6.4.5 Configuring Priorities

Configuration Effect

- Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.
- Configure the port priority to determine which port enters the forwarding state.

Notes

- It is recommended to set the priority of the core device higher (to a smaller value) to ensure stability of the entire network. You can assign different switch priorities to different instances so that each instance runs an independent STP based on the assigned priorities. Devices in different regions use the priority only of the CIST (Instance 0). As described in bridge ID, the switch priority has 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096. The default value is 32,768.
- If two ports are connected to a shared device, the device selects a port with a higher priority (smaller value) to enter the forwarding state and a port with a lower priority (larger value) to enter the discarding state. If the two ports have the same priority, the device selects the port with a smaller port ID to enter the forwarding state. You can assign different port priorities to different instances on a port so that each instance runs an independent STP based on the assigned priorities.
- Similar to the switch priority, the port priority also has 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 16. The default value is 128.

Configuration Steps

Configuring the Switch Priority

- Optional.
- To change the root or topology of a network, configure the switch priority.

Command	**spanning-tree** [**mst** *instance-id*] **priority** *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **priority** *priority*: Indicates the switch priority. There are 16 optional values: 0, 4,096, 8,192, 12,288, 16,384, 20,480, 24,576, 28,672, 32,768, 36,864, 40,960, 45,056, 49,152, 53,248, 57,344, 61,440. They are integral multiples of 4,096.
Command Mode	Global configuration mode
Usage Guide	Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuring the Port Priority

- Optional.
- To change the preferred port entering the forwarding state, configure the port priority.

Command	spanning-tree [**mst** *instance-id*] **port-priority** *priority*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **port-priority** *priority*: Indicates the port priority. There are 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. They are integral multiples of 4,096.
Command Mode	Interface configuration mode
Usage Guide	If a loop occurs in a region, the port with a higher priority is preferred to enter the forwarding state. If two ports have the same priority, the port with a smaller port ID is selected to enter the forwarding state. Run this command to determine which port in the loop of a region enters the forwarding state.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Priority

Scenario **Figure 6-22**	
Configuration Steps	● Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ● Configure the priority of Gi0/2 on DEV A is 16 so that Gi0/2 on DEV B can be selected as the root port.
DEV A	Step 1: Enable STP and configure the bridge priority. `Ruijie(config)#spanning-tree` `Ruijie(config)#spanning-tree mst 0 priority 0` Step 2: Configure the priority of Gi 0/2. `Ruijie(config)# int gi 0/2` `Ruijie(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16`
DEV B	`Ruijie(config)#spanning-tree`
Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.
DEV A	`Ruijie# Ruijie#show spanning-tree summary` `Spanning tree enabled protocol mstp` `MST 0 vlans map : ALL` `  Root ID    Priority    0` `             Address     00d0.f822.3344` `             this bridge is root` `             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec` `  Bridge ID  Priority    0` `             Address     00d0.f822.3344` `             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`

	Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 16 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	Ruijie#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 001a.a917.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Root FWD 20000 128 False P2p Gi0/1 Altn BLK 20000 128 False P2p

Common Errors

The port priority will take effect only after the designated port has been changed.

6.4.6 Configuring the Port Path Cost

Configuration Effect

- Configure the path cost of a port to determine the forwarding state of the port and the topology of the entire network.
- If the path cost of a port uses its default value, configure the path cost calculation method to affect the calculation result.

Notes

- A device selects a port as the root port if the path cost from this port to the root bridge is the lowest. Therefore, the port path cost determines the root port of the local device. The default port path cost is automatically calculated based on the port rate (Media Speed). A port with a higher rate will have a low path cost. Since this method can calculate the most scientific path cost, do not change the path cost unless required. You can assign different path costs to different instances on a port so that each instance runs an independent STP based on the assigned path costs.
- If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate. However, IEEE 802.1d-1998 and IEEE 802.1t define different path costs for the same link rate. The value is a short integer ranging from 1 to 65,535 in 802.1d-1998 while is a long integer ranging from 1 to 200,000,000 in IEEE 802.1t. The path cost of an aggregate port (AP) has two solutions: 1. Ruijie solution: Port Path Cost x 95%; 2. Solution recommended in standards: 20,000,000,000/Actual link bandwidth of the AP, in which Actual link bandwidth of the AP = Bandwidth of a member port x Number of active member ports. The administrator must unify the path cost calculation method in the entire network. The default standard is the private long integer standard.
- The following table lists path costs automatically configured for different link rate in two solutions.

Port Rate	Port	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (long standard)
10M	Common port	100	2000000	2000000
	AP	95	1900000	2000000÷linkupcnt
100M	Common port	19	200000	200000
	AP	18	190000	200000÷linkupcnt
1000M	Common port	4	20000	20000
	AP	3	19000	20000÷linkupcnt
10000M	Common port	2	2000	2000
	AP	1	1900	20000÷linkupcnt

- Ruijie's long integer standard is used by default. After the solution is changed to the path cost solution recommended by the standards, the path cost of an AP changes with the number of member ports in UP state. If the port path cost changes, the network topology also will change.
- If an AP is static, linkupcnt in the table is the number of active member ports. If an AP is an LACP AP, linkupcnt in the table is the number of member ports forwarding AP data. If no member port in the AP goes up, linkupcnt is 1. For details about AP and LACP, see the *Configuring AP*.

Configuration Steps

Configuring the Port Path Cost

- Optional.
- To determine which port or path data packets prefer to pass through, configure the port path cost.

Command	**spanning-tree** [**mst** *instance-id*] **cost** *cost*
Parameter Description	**mst** *instance-id*: Indicates the instance ID, ranging from 0 to 64. **cost** *cost*: Indicates the path cost, ranging from 1 to 200,000,000.

Command Mode	Interface configuration mode
Usage Guide	A larger value of *cost* indicates a higher path cost.

Configuring the Default Path Cost Calculation Method

- Optional.
- To change the path cost calculation method, configure the default path cost calculation method.

Command	**spanning-tree pathcost method** { *long* [*standard*] | *short* }
Parameter Description	*long*: Uses the path cost specified in 802.1t. *standard*: Uses the cost calculated according to the standard. *short*: Uses the path cost specified in 802.1d.
Command Mode	Global configuration mode
Usage Guide	If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Path Cost

Scenario Figure 6-23	
Configuration Steps	● Configure the bridge priority so that DEV A becomes the root bridge of the spanning tree. ● Configure the path cost of Gi 0/2 on DEV B is 1 so that Gi 0/2 can be selected as the root port.
DEV A	`Ruijie(config)#spanning-tree` `Ruijie(config)#spanning-tree mst 0 priority 0`

DEV B	Ruijie(config)#spanning-tree Ruijie(config)# int gi 0/2 Ruijie(config-if-GigabitEthernet 0/2)# spanning-tree cost 1
Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.
DEV A	Ruijie# Ruijie#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 0 Address 00d0.f822.3344 Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	Ruijie#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

```
  Bridge ID  Priority    32768
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec


Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Root FWD 1          128      False    P2p
Gi0/1            Altn BLK 20000      128      False    P2p
```

Common Errors

The changed port path cost will take effect only on the Rx port.

6.4.7 Configuring the Maximum Hop Count of a BPDU Packet

Configuration Effect

- Configure the maximum hop count of a BPDU packet to change the BPDU TTL and thereby affect the network topology.

Notes

- The default maximum hop count of a BPDU packet is 20. Generally, it is not recommended to change the default value.

Configuration Steps

↘ Configuring the Maximum Hop Count

- (Optional) If the network topology is so large that a BPDU packet exceeds the default 20 hops, it is recommended to change the maximum hop count.

Command	**spanning-tree max-hops** *hop-count*
Parameter Description	*hop-count*: Indicates the number of devices a BPDU passes through before being discarded. It ranges from 1 to 40.
Command Mode	Global configuration mode
Usage Guide	In a region, the BPDU sent by the root bridge includes a hop count. Every time a BPDU passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU times out and the device discards the packet. This command specifies the number of devices a BPDU passes through in a region before being discarded. Changing the maximum hop count will affect all instances.

Verification

- Display the configuration.

Configuration Example

Configuring the Maximum Hop Count of a BPDU Packet

Configuration Steps	● Set the maximum hop count of a BPDU packet to 25.
	`Ruijie(config)# spanning-tree max-hops 25`
Verification	● Run the **show spanning-tree** command to display the configuration.
	`Ruijie# show spanning-tree` `StpVersion : MSTP` `SysStpStatus : ENABLED` `MaxAge : 20` `HelloTime : 2` `ForwardDelay : 15` `BridgeMaxAge : 20` `BridgeHelloTime : 2` `BridgeForwardDelay : 15` `MaxHops: 25` `TxHoldCount : 3` `PathCostMethod : Long` `BPDUGuard : Disabled` `BPDUFilter : Disabled` `LoopGuardDef : Disabled` `###### mst 0 vlans map : ALL` `BridgeAddr : 00d0.f822.3344` `Priority: 0` `TimeSinceTopologyChange : 2d:0h:46m:4s` `TopologyChanges : 25` `DesignatedRoot : 0.001a.a917.78cc` `RootCost : 0` `RootPort : GigabitEthernet 0/1` `CistRegionRoot : 0.001a.a917.78cc`

	CistPathCost : 20000

6.4.8 Enabling PortFast-related Features

Configuration Effect

- After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.
- If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
- If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Notes

- The global BPDU guard takes effect only when PortFast is enabled on a port.
- If BPDU filter is enabled globally, a PortFast-enabled port neither sends nor receives BPDUs. In this case, the host connecting directly to the PortFast-enabled port does not receive any BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically fails.
- The global BPDU filter takes effect only when PortFast is enabled on a port.

Configuration Steps

Enabling PortFast

- Optional.
- If a port connects directly to the network terminal, configure this port as a PortFast port.

Command	**spanning-tree portfast**
Parameter Description	N/A
Defaults	PortFast is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

Enabling BPDU Guard

- Optional.
- If device ports connect directly to network terminals, you can enable BPDU guard on these ports to prevent BPDU attacks from causing abnormality in the spanning tree topology. A port enabled with BPDU guard enters the error-disabled state after receiving a BPDU.

- If device ports connect directly to network terminals, you can enable BPDU guard to prevent loops on the ports. The prerequisite is that the downlink device (such as the hub) can forward BPDU packets.

Command	**spanning-tree portfast bpduguard default**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU. Run the **show spanning-tree** command to display the configuration.

Enabling BPDU Guard on an Interface

Command	**spanning-tree bpduguard enabled**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.

Enabling BPDU Filter

- Optional.
- To prevent abnormal BPDU packets from affecting the spanning tree topology, you can enable BPDU filter on a port to filter abnormal BPDU packets.

Command	**spanning-tree portfast bpdufilter default**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If BPDU filter is enabled, corresponding ports neither send nor receive BPDUs.

Enabling BPDU Filter on an Interface

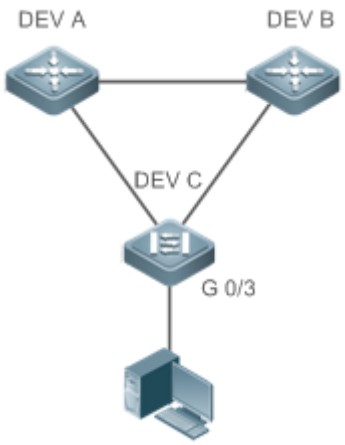
Command	**spanning-tree bpdufilter enabled**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Verification

- Display the configuration.
- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Enabling PortFast on a Port

Scenario **Figure 6-24**	
Configuration Steps	● Configure Gi 0/3 of DEV C as a PortFast port and enable BPDU guard.
DEV C	`Ruijie(config)# int gi 0/3` `Ruijie(config-if-GigabitEthernet 0/3)# spanning-tree portfast` `%Warning: portfast should only be enabled on ports connected to a single` `host. Connecting hubs, switches, bridges to this interface when portfast is` `enabled,can cause temporary loops.` `Ruijie(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable`
Verification	● Run the **show spanning-tree interface** command to display the port configuration.
DEV C	`Ruijie#show spanning-tree int gi 0/3` `PortAdminPortFast : Enabled` `PortOperPortFast : Enabled` `PortAdminAutoEdge : Enabled` `PortOperAutoEdge : Enabled` `PortAdminLinkType : auto`

```
PortOperLinkType : point-to-point

PortBPDUGuard : Enabled

PortBPDUFilter : Disabled

PortGuardmode  : None


###### MST 0 vlans mapped :ALL

PortState : forwarding

PortPriority : 128

PortDesignatedRoot : 0.00d0.f822.3344

PortDesignatedCost : 0

PortDesignatedBridge :0.00d0.f822.3344

PortDesignatedPortPriority : 128

PortDesignatedPort : 4

PortForwardTransitions : 1

PortAdminPathCost : 20000

PortOperPathCost : 20000

Inconsistent states : normal

PortRole : designatedPort
```

6.4.9 Enabling TC-related Features

Configuration Effect

- If TC protection is enabled on a port, the port deletes TC BPDU packets within a specified time (generally 4 seconds) after receiving them, preventing MAC and ARP entry from being removed.
- If TC guard is enabled, a port receiving TC packets filters TC packets received or generated by itself so that TC packets are not spread to other ports. In this way, possible TC attacks are efficiently prevented to keep the network stable.
- TC filter does not process TC packets received by ports but processes TC packets in case of normal topology changes.

Notes

- It is recommended to enable TC guard only when illegal TC attack packets are received in the network.

Configuration Steps

↘ Enabling TC Protection

- Optional.

- TC protection is disabled by default.

Command	spanning-tree tc-protection
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling TC Guard

- Optional.
- TC guard is disabled by default.
- To filter TC packets received or generated due to topology changes, you can enable TC guard.

Command	spanning-tree tc-protection tc-guard
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Enabling TC Guard on an Interface

Command	spanning-tree tc-guard
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable TC guard to prevent TC packets from spreading.

Enabling TC Filter

- Optional.
- TC filter is disabled by default.
- To filter TC packets received on a port, you can enable TC filter on the port.

Command	spanning-tree ignore tc
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If TC filter is enabled on a port, the port does not process received TC packets.

Verification

- Display the configuration.

Configuration Example

Enabling TC Guard on a Port

Configuration Steps	Enable TC guard on a port.
	`Ruijie(config)#int gi 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard`
Verification	• Run the **show run interface** command to display the TC guard configuration of the port.
	`Ruijie#show run int gi 0/1` `Building configuration...` `Current configuration : 134 bytes` `interface GigabitEthernet 0/1` ` switchport mode trunk` ` spanning-tree tc-guard`

Common Errors

- If TC guard or TC filter is incorrectly configured, an error may occur during packet forwarding of the network device. For example, when the topology changes, the device fails to clear MAC address in a timely manner, causing packet forwarding errors.

6.4.10 Enabling BPDU Source MAC Address Check

Configuration Effect

- Enable BPDU source MAC address check. After this, a device receives only BPDU packets with the source MAC address being the specified MAC address and discards other BPDU packets.

Notes

- When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check so that the switch receives the BPDU packets sent only by the peer switch.

Configuration Steps

Enabling BPDU Source MAC Address Check

- Optional.

- To prevent malicious BPDU attacks, you can enable BPDU source MAC address check.

Command	**bpdu src-mac-check** *H.H.H*
Parameter Description	*H.H.H*: Indicates an MAC address. The device receives only BPDU packets with this address being the source MAC address.
Command Mode	Interface configuration mode
Usage Guide	BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Source MAC Address Check on a Port

Configuration Steps	Enable BPDU source MAC address check on a port.
	`Ruijie(config)#int gi 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234`
Verification	• Run the **show run interface** command to display the spanning tree configuration of the port.
	`Ruijie#show run int gi 0/1` `Building configuration...` `Current configuration : 170 bytes` `interface GigabitEthernet 0/1` ` switchport mode trunk` ` bpdu src-mac-check 00d0.f800.1234` `spanning-tree link-type point-to-point`

Common Errors

- If BPDU source MAC address check is enabled on a port, the port receives only BPDU packets with the configured MAC address being the source MAC address and discards all other BPDU packets.

6.4.11 Configuring Auto Edge

Configuration Effect

- Enable Auto Edge. If a designated port does not receive any BPDUs within a specified time (3 seconds), it is automatically identified as an edge port. However, if the port receives BPDUs, its Port Fast Operational State will become Disabled.

Notes

- Unless otherwise specified, do not disable Auto Edge.

Configuration Steps

Configuring Auto Edge

- Optional.
- Auto Edge is enabled by default.

Command	spanning-tree autoedge
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU. You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

Verification

- Display the configuration.

Configuration Example

Disabling Auto Edge on a Port

Configuration Steps	Disable Auto Edge on a port.
	`Ruijie(config)#int gi 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled`
Verification	• Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
	`Ruijie#show spanning-tree interface gi 0/1`

```
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Disabled
PortOperAutoEdge : Disabled
PortAdminLinkType : point-to-point
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : None

###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.00d0.f822.3344
PortDesignatedCost : 0
PortDesignatedBridge :0.00d0.f822.3344
PortDesignatedPortPriority : 128
PortDesignatedPort : 2
PortForwardTransitions : 6
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
```

Common Errors

If packet loss or Rx/Tx message delay exists, it is recommended to disable Auto Edge function.

6.4.12 Enabling Guard-related Features

Configuration Effect

- If root guard is enabled on a port, its roles on all instances are enforced as the designated port. Once the port receives configuration information with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive configuration information with a higher priority within a period, it returns to its original state.

- Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is to prevent this problem.

Notes

- Root guard and loop guard cannot take effect on a port at the same time.

Configuration Steps

Enabling Root Guard

- Optional.
- The root bridge may receive configuration with a higher priority due to incorrect configuration by maintenance personnel or malicious attacks in the network. As a result, the current root bridge may lose its role, causing incorrect topology changes. To prevent this problem, you can enable root guard on a designated port of a device.

Command	spanning-tree guard root
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.

Enabling Loop Guard

- Optional.
- You can enable loop guard on a port (root port, master port, or AP) to prevent it from failing to receive BPDUs sent by the designated bridge, increasing device stability. Otherwise, the network topology will change, possibly causing a loop.

Command	spanning-tree loopguard default
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

Enabling Loop Guard on an Interface

Command	spanning-tree guard loop
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt

	failure.

Disabling Guard

- Optional.

Command	**spanning-tree guard none**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Display the configuration.

Configuration Example

Enabling Loop Guard on a Port

Scenario Figure 6-25	
Configuration Steps	• Configure DEV A as the root bridge and DEV B as a non-root bridge on a spanning tree. • Enable loop guard on ports Gi 0/1 and Gi 0/2 of DEV B.
DEV A	`Ruijie(config)#spanning-tree` `Ruijie(config)#spanning-tree mst 0 priority 0`
DEV B	`Ruijie(config)#spanning-tree` `Ruijie(config)# int range gi 0/1-2` `Ruijie(config-if-range)#spanning-tree guard loop`
Verification	• Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
DEV A	`Omitted.`

DEV B	Ruijie#show spanning-tree int gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Disabled PortAdminLinkType : auto PortOperLinkType : point-to-point PortBPDUGuard : Disabled PortBPDUFilter : Disabled PortGuardmode : Guard loop ###### MST 0 vlans mapped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.001a.a917.78cc PortDesignatedCost : 0 PortDesignatedBridge :0.001a.a917.78cc PortDesignatedPortPriority : 128 PortDesignatedPort : 17 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : rootPort Ruijie#show spanning-tree int gi 0/2 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Enabled

```
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : Guard loop

###### MST 0 vlans mapped :ALL
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 18
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : alternatePort
```

Common Errors

- If root guard is enabled on the root port, master port, or AP, the port may be incorrectly blocked.

6.4.13 Enabling BPDU Transparent Transmission

Configuration Effect

- If STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated.

Notes

- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Configuration Steps

Enabling BPDU Transparent Transmission

- Optional.
- If STP is disabled on a device that needs to transparently transmit BPDU packets, enable BPDU transparent transmission.

Command	bridge-frame forwarding protocol bpdu
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliant with IEEE 802.1Q do not forward the BPDU packets received. However, devices may need to transparently transmit BPDU packets in actual network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDU packets so that the spanning tree between devices is properly calculated. BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDU packets.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Transparent Transmission

Scenario Figure 6-26	
	STP is enabled on DEV A and DEV C while is disabled on DEV B.
Configuration Steps	• Enable BPDU transparent transmission on DEV B so that STP between DEV A and DEV C can be correctly calculated.
DEV B	`Ruijie(config)#bridge-frame forwarding protocol bpdu`
Verification	• Run the **show run** command to check whether BPDU transparent transmission is enabled.
DEV B	`Ruijie#show run` `Building configuration...` `Current configuration : 694 bytes` `bridge-frame forwarding protocol bpdu`

6.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the statistics of packets sent and received on a port.	**clear spanning-tree counters** [**interface** *interface-id*]
Clears the STP topology change information.	**clear spanning-tree mst** *instance-id* **topochange record**

Displaying

Description	Command
Displays MSTP parameters and spanning tree topology information.	**show spanning-tree**
Displays the count of sent and received MSTP packets.	**show spanning-tree counters** [**interface** *interface-id*]
Displays MSTP instances and corresponding port forwarding status.	**show spanning-tree summary**
Displays the ports that are blocked by root guard or loop guard.	**show spanning-tree inconsistentports**
Displays the configuration of an MST region.	**show spanning-tree mst configuration**
Displays MSTP information of an instance.	**show spanning-tree mst** *instance-id*
Displays MSTP information of the instance corresponding to a port.	**show spanning-tree mst** *instance-id* **interface** *interface-id*
Displays topology changes of a port in an instance.	**show spanning-tree mst** *instance-id* **topochange record**
Displays MSTP information of all instances corresponding to a port.	**show spanning-tree interface** *interface-id*
Displays the forwarding time.	**show spanning-tree forward-time**
Displays the hello time.	**show spanning-tree hello time**
Displays the maximum hop count.	**show spanning-tree max-hops**
Displays the maximum number of BPDU packets sent per second.	**show spanning-tree tx-hold-count**
Displays the path cost calculation method.	**show spanning-tree pathcost method**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs all STPs.	**debug mstp all**
Debugs MSTP Graceful Restart (GR).	**debug mstp gr**

Debugs BPDU packet receiving.	**debug mstp rx**
Debugs BPDU packet sending.	**debug mstp tx**
Debugs MSTP events.	**debug mstp event**
Debugs loop guard.	**debug mstp loopguard**
Debugs root guard.	**debug mstp rootguard**
Debugs the bridge detection state machine.	**debug mstp bridgedetect**
Debugs the port information state machine.	**debug mstp portinfo**
Debugs the port protocol migration state machine.	**debug mstp protomigrat**
Debugs MSTP topology changes.	**debug mstp topochange**
Debugs the MSTP receiving state machine.	**debug mstp receive**
Debugs the port role transition state machine.	**debug mstp roletran**
Debugs the port state transition state machine.	**debug mstp statetran**
Debugs the MSTP sending state machine.	**debug mstp transmit**

7 Configuring VLAN Group

7.1 Overview

Each virtual LAN (VLAN) group contains multiple VLANs. VLAN group function associates a wireless LAN (WLAN) with a VLAN group, achieving 1:N mapping between them, which assigns VLANs flexibly to WLAN-accessed stations (STAs).

VLAN assignment mode:

- After STAs pass 802.1X authentication, the authentication server assigns VLANs to STAs.

Protocols and Standards

- N/A

7.2 Applications

Application	Description
VLAN Assignment	The VLAN group assigns VLANs to WLAN-associated STAs.

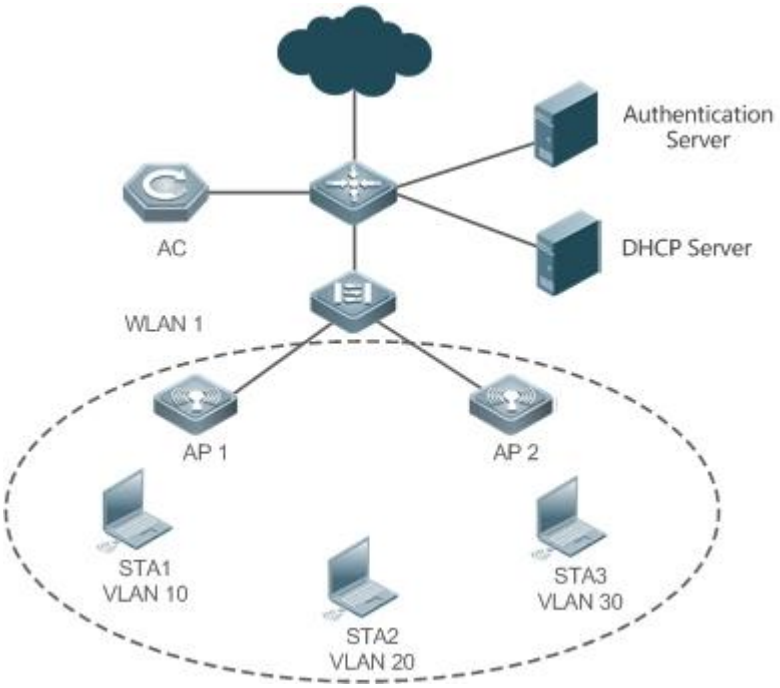
7.2.1 VLAN Assignment

Scenario

Multiple STAs access the same WLAN. VLANs are assigned to STAs based on the VLAN assignment mode of the VLAN group mapped to the current WLAN.

As shown in Figure 7-1, the VLAN group assigns VLANs to STA 1, STA 2, and STA 3 that have accessed WLAN 1.

Figure 7-1



Remarks	STA is a wireless device. AP 1 and AP 2 are the access points through which STAs access the wired network. AC is a wireless access controller. It connects with APs through the wired network to manage APs in a unified manner. WLAN 1 is a wireless local area network.

7.3 Features

Basic Concepts

VLAN Group

Multiple VLANs are added to a VLAN group. When STAs access a WLAN, VLANs are assigned to the STAs based on the VLAN assignment mode of the VLAN group mapped to the current WLAN.

VLAN Assignment Mode

Each VLAN group can assign VLANs based on 802.1X.

Overview

Feature	Description

802.1X-based VLAN Assignment	You can plan VLANs to be assigned after STAs pass 802.1X authentication.

7.3.1 802.1X-based VLAN Assignment

Working Principle

Before authentication, an STA belongs to the default VLAN of a VLAN group mapped to the currently accessed WLAN.

The STA will be authenticated in the default VLAN. After authentication succeeds, the authentication server determines whether to assign a VLAN. If yes, the packets subsequently sent by the STA will be automatically redirected to the assigned VLAN. If no, the packets will be transmitted in the default VLAN of the VLAN group.

7.4 Configuration

Configuration	Description and Command	
Configuring a VLAN Group	⚠ (Mandatory) It is used to create a VLAN group and configure a VLAN list, the VLAN assignment mode, and default VLAN.	
	vlan-group *group-id*	Creates a VLAN group.
	vlan-list *vlan-list*	Configures a VLAN list for a VLAN group.
	vlan-assign-mode XX	Specifies the VLAN assignment mode for a VLAN group.
	default-vlan XX	Configures the default VLAN for a VLAN group.
Configuring WLAN-VLAN Group Mapping	⚠ (Mandatory) It is used to configure the mapping between a WLAN and a VLAN group.	
	vlan-group *group-id*	Configures WLAN-VLAN group mapping on APs.
	interface-mapping *wlan-id* **group** *group-id*	Configures WLAN-VLAN group mapping on ACs.

7.4.1 Configuring a VLAN Group

Configuration Effect

- Create a VLAN group and complete configurations related to the VLAN group.

Notes

- N/A

Configuration Steps

↘ **Creating a VLAN Group**

- Mandatory.

Configuring a VLAN List for a VLAN Group

- Mandatory. Ensure that VLANs have been created.

Configuring the VLAN Assignment Mode for a VLAN Group

- Mandatory.
- Use this command to implement the VLAN assignment policy of a VLAN group.

Configuring the Default VLAN for a VLAN Group

- Mandatory in 802.1X-based assignment mode.
- The default VLAN takes effect when the current WLAN is in 802.1X-based assignment mode, that is, when the authentication server assigns the default VLAN before 802.1X authentication succeeds.

Verification

- Check the configurations of the VLAN group.

Configuration Example

Configuring a VLAN Group

Configuration Steps	• Create VLAN Group 10. • Set the VLAN assignment mode to 802.1X-based mode. • Configure a VLAN list that contains VLAN 1 to VLAN 10. • Set the default VLAN to VLAN 1.
	Ruijie# configure terminal Ruijie(config)# vlan-group 10 Ruijie(config-vlan-group)# vlan-assign-mode dot1x Ruijie(config-vlan-group)# vlan-list 1-10 Ruijie(config-vlan-group)# default-vlan 1 Ruijie(config-vlan-group)# end
Verification	• Check whether the configurations of VLAN Group 10 are correct.
	Ruijie#show vlan-group 10 vlan-group id mode default-vlan vlan-list ------------ ---------- ---------- ---------- 10 dot1x 1 1-10

Common Errors

- A VLAN configured in a VLAN list does not exist.
- The default VLAN configured does not exist in the VLAN list.

⚠ The ID of a created VLAN group ranges from 1 to 128.

A VLAN group contains a maximum of 128 VLANs.

7.4.2 Configuring WLAN-VLAN Group Mapping

Configuration Effect

- Configure the mapping between a WLAN and a VLAN group so that STAs can be associated with the WLAN.

Notes

- N/A

Configuration Steps

Configure WLAN-VLAN Group Mapping

- Mandatory.

Verification

- Check whether the mapping between a WLAN and a VLAN group is correct.

Configuration Example

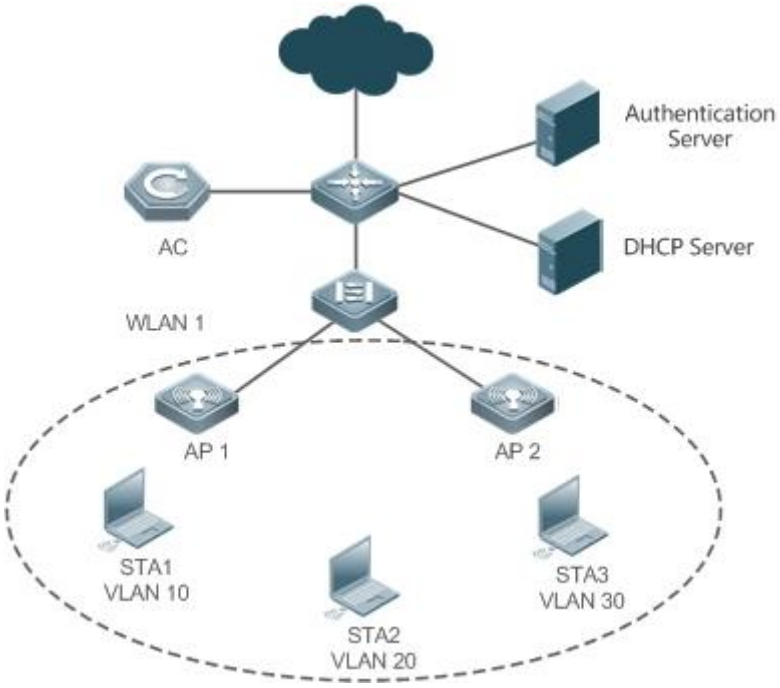
Configure WLAN-VLAN Group Mapping on ACs

Configuration Steps	• Enter the AP group configuration mode. • Configure the WLAN-VLAN group mapping.
	`Ruijie(config)# ap-group default` `Ruijie(config-ap-group)# interface-mapping 100 vlan-group 100`
Verification	• Run the **show running** command to check whether the configurations are correct.

Configuration Example of 802.1X-based VLAN Assignment

In the WLAN scenario shown in Figure 7-2, leaders, employees, and visitors are differentiated to access the WLAN with different privilege levels. The following configurations are required:

- Create VLAN Group 100, including VLAN 10, VLAN 20, and VLAN 30.
- Map WLAN 1 to VLAN Group 100. When STAs access WLAN 1, the authentication server performs 802.1X authentication for the STAs. After the authentication is complete, the authentication server assigns VLAN 10 to leaders, VLAN 20 to employees, and VLAN 30 to visitors.

Scenario **Figure 7-2**	
Configuration Steps	● If the WLAN-VLAN mapping is 1:N, different VLANs can be assigned to STAs in the same WLAN. ● Set the WLAN authentication mode to 802.1X authentication so that different VLANs can be assigned to different STAs.
AP1 & AP2 **AC**	APs apply the centralized forwarding in fit AP architecture by default, and are managed by ACs in a unified manner. Step 1: Create VLANs respectively for different types of users. Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# vlan range 10 , 20 , 30 Ruijie(config-vlan-range)# exit Step 2: Create a VLAN group, add VLAN 10, VLAN 20, and VLAN 30 to the group, and configure VLAN 30 as the default VLAN for visitors. Ruijie(config)# vlan-group 100 Ruijie(config-vlan-group)# vlan-assign-mode dot1x Ruijie(config-vlan-group)# vlan-list 10 , 20 , 30 Ruijie(config-vlan-group)# default-vlan 30 Ruijie(config-vlan-group)# exit Step 3: Create WLAN 1, with the WLAN authentication mode set to 802.1X authentication and the encryption mode set to Advanced Encryption Standard (AES). Ruijie(config)# wlan-config 1 office_wifi Ruijie(config-wlan)# exit Ruijie(config)# wlansec 1

Authentication Server	Ruijie(wlansec)# security wpa enable Ruijie(wlansec)# security wpa akm 802.1x enable Ruijie(wlansec)# security wpa ciphers aes enable Step 4: Configure the mapping between WLAN 1 and VLAN Group 100. Ruijie(config)# ap-group default Ruijie(config-ap-group)# interface-mapping 1 vlan-group 100 Before establishing a new STA type on the authentication server, you need to configure a specific VLAN for the assignment.
Verification	● Check the VLAN group configurations on the AC.
AC	Ruijie# show vlan-group VLAN-Group ID Default VLAN Assign-Mode VLAN-List ---------- ---------- ---------- ---------- 100 30 dot1x 10，20，30

Common Errors

- N/A

7.5 Monitoring

Clearing

N/A

Displaying

Description	Command
Displays the VLAN group information.	**show vlan-group** [*group-id*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the VLAN group status.	**debug bridge vgoup**

8 Configuring PPPoE-CLIENT

8.1 Overview

PPPoE: Point-to-point Protocol Over Ethernet

Ruijie products support the PPPoE client on Ethernet interfaces, and are therefore able to connect to a host network by accessing a remote hub through a simple access device. The PPPoE protocol enables the PPPoE server to control each access client and perform relevant accounting.

Ruijie products support two dialing modes: Dial-on-Demand Routing (DDR) mode and no Dial-on-Demand Routing (DDR) but always online.

- The PPPoE client is applicable in scenarios where Internet access is implemented through ADSL.

The following sections describe the PPPoE client only.

Protocols and Standards

- RFC2516: A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC1661: The Point-to-Point Protocol (PPP)

8.2 Applications

Application	Description
ADSL Scenario	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

8.2.1 ADSL Scenario

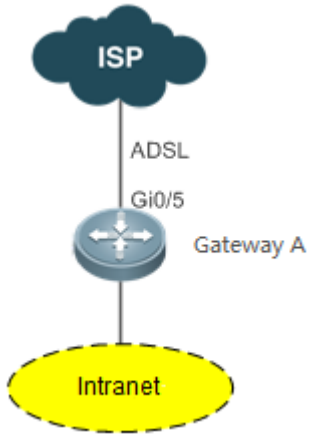
Scenario

In a scenario where Internet access is implemented through ADSL, the device provides dialup and packet forwarding functions.

The dialup networking scenario is illustrated with Figure 8-1 as an example.

- The dialup function is enabled on the device. The device connects to a remote Internet service provider (ISP) over an ADSL line, and obtains Internet access capability.
- Intranet PCs access the Internet through the device.

Figure 8-1



Corresponding Protocols

- Enable the dialup function on the device, and dial up to the Internet over the ADSL line.

8.3 Features

Basic Concepts

ISP

A network operator who provides users with Internet access service, information service, and value-added services (VASs).

ADSL

A line on which users dial up to the Internet.

Data Flow

A flow of packets only forwarded by the device.

Interested Flow

A specific type of packets defined by users during configuration, which can trigger the device to start dialup.

Overview

Feature	Description
Dialup to the Internet	In a scenario where Internet access is implemented through the Asymmetric Digital Subscriber Line (ADSL) technology, the device provides dialup and packet forwarding functions.

8.3.1 Dialup to the Internet

The device has Internet access capability after the dialup is complete; therefore, hosts in the intranet also have Internet access capability.

Working Principle

Dialup corresponds to the negotiation process, whereas Internet access corresponds to the packet forwarding process.

Negotiation can be further divided into three parts: protocol negotiation, protocol keepalive, and protocol termination.

Protocol Negotiation

Protocol negotiation is divided into PPPoE negotiation and PPP negotiation.

During PPPoE negotiation, both parties confirm a unique peer, record the peer's MAC address, and establish a unique session ID.

During PPP negotiation, the server checks the client's authentication information. If the client passes the authentication, the server allocates an IP address to the client. If the client has already been configured with an IP address and the configured IP address meets the server's requirements, the server will agree to use this IP address as the IP address of the client.

After both protocols are up, the device has Internet access capability and prepares a Layer 2 (L2) header that is necessary for data packet encapsulation.

Protocol Keepalive

After PPP is up, both parties periodically send LCP heartbeat packets to each other. If the party at one end does not receive any heartbeat response from the other party, it actively terminates the protocol.

Protocol Termination

In certain cases, either party may actively terminate the protocol.

The initiating party sends a PPP termination packet to end the current PPP session, and then sends a PPPoE termination packet to end the current PPPoE session.

After receiving the PPP termination packet, the passive party returns an acknowledgement packet to agree to the termination of the PPP session; and after receiving the PPPoE termination packet, the passive party returns another acknowledgement packet to agree to the termination of the PPPoE session.

Once either party receives a PPPoE termination protocol, the PPP session and the PPPoE session will immediately terminate, even if it has not received any PPP termination protocol.

Packet Forwarding

Packet sending process: When a data packet is routed to the dialer interface, the device encapsulates the data packet with the prepared L2 header information and ultimately sends the data packet from a physical port.

Packet receiving process: After a packet arrives at a physical port, the device marks the Layer 3 (L3) header position of the packet, executes the next service, and ultimately sends the packet to a host in the intranet.

Related Configuration

Configuring the Ethernet Interface

By default, the following functions are disabled and there is no corresponding default value.

Run the **pppoe enable** command to enable the PPPoE client function on the interface.

Run the **no pppoe enable** command to disable the PPPoE client function on the interface.

Run the **pppoe-client dial-pool-number** *pool-number* command to bind the Ethernet interface to a specific logical dialer pool.

Run the **no pppoe-client dial-pool-number** *pool-number* command to unbind the Ethernet interface from the specific logical dialer pool.

Configuring the Logical Interface

By default, the following functions are disabled.

Run the **interface dialer** *dialer-number* command to add a specific logical interface and enter the configuration mode of the logical interface.

Run the **no interface dialer** *dialer-number* command to delete the specific logical interface.

Run the **ip address negotiate** command to configure negotiation-based IP address acquisition.

Run the **no ip address negotiate** command to remove the configuration of negotiation-based IP address acquisition.

Run the **dialer pool** *number* command to associate a dialer pool, which corresponds to the dialer pool configured on the Ethernet interface.

Run the **no dialer pool** *number* command to remove the association with the dialer pool.

Run the **encapsulation ppp** command to configure the encapsulation protocol PPP. PPPoE is established on the basis of PPP.

Run the **no encapsulation** command to remove the encapsulation protocol configuration.

Run the **mtu** *1488* command to set the Maximum Transmit Unit (MTU) to 1488.

Run the **no mtu** command to remove the MTU configuration.

Run the **dialer-group** *dialer-group-number* command to associate a dialer triggering rule, which corresponds to the dialer-list.

Run the **no dialer-group** command to remove the configuration of the dialer triggering rule.

Run the **ppp chap hostname** *username* command to configure the user name for CHAP authentication.

Run the **no ppp chap hostname** command to remove the user name configuration for CHAP authentication.

Run the **ppp chap password** *password* command to configure the password for CHAP authentication.

Run the **no ppp chap password** command to remove the password configuration for CHAP authentication.

Run the **ppp pap sent-username** *username* **password** *password* command to configure the user name and password for PAH authentication.

Run the **no ppp pap sent-username** command to remove the user name and password configuration for PAH authentication.

Configuring Mandatory Global Parameters

By default, the following functions are disabled and shall be configured according to actual requirements. If other functional modules need to be used together, you also need to configure other global parameters.

Run the **dialer-list number protocol** *protocol-name* { **permit** | **deny** | **list** *access-list-number* } command to define a dialer triggering rule.

Run the **no dialer-list number** command to delete the configured dialer triggering rule.

Run the **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* [**permanent**] command to configure a route. If you specify the **permanent** option, the route will be always valid, even if the logical interface is within the enable-timeout period, in which case the logical interface will be down.

Run the **no ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* command to remove the route.

8.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of the PPPoE Client	Mandatory configuration.	
	pppoe enable	Enables the PPPoE client function.
	pppoe-client dial-pool-number *number* { **dial-on-demand** | **no-ddr**	Binds a logical dialer pool and specifies the dialing mode.
	interface dialer *dialer-number*	Adds a specific logical interface and enters the configuration mode of the logical interface.
	ip address { **negotiate** | *ip-addr subnet-mask* }	Configures the IP address acquisition mode.
	dialer pool *number*	Associates a dialer pool.
	encapsulation ppp	Configures the encapsulation protocol PPP.
	mtu *1488*	Sets the MTU to 1488.
	dialer-group *dialer-group-number*	Associates a dialer triggering rule.
	ppp chap hostname *username*	Configures the user name for CHAP authentication.
	ppp chap password *password*	Configures the password for CHAP authentication.
	ppp pap sent-username *username* **password** *password*	Configures the user name and password for PAP authentication.
	dialer-list number protocol *protocol-name* { **permit** | **deny** | **list** *access-list-number* }	Defines a dialer triggering rule.

8.4.1 Configuring Basic Functions of the PPPoE Client

Networking Requirements

- The device initiates PPPoE negotiation, and completes the negotiation process, protocol keepalive, and protocol termination.
- The device obtains Internet access capability after the negotiation is complete, and starts to forward a data flow which is routed to the dialer interface.

Notes

- After the kernel module is uninstalled, users can still perform configuration management but negotiation and data flow forwarding cannot be performed.

Configuration Steps

Enabling the PPPoE Client Function

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Enable the PPPoE client function.

Binding a Logical Dialer Pool and Specifying the Dialing Mode

- The configuration is mandatory.
- Perform this configuration in Ethernet interface configuration mode.
- Bind the Ethernet interface to a specific logical dialer pool and specify the dialer mode.

Adding a Specific Logical Interface and Entering the Configuration Mode of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Add a specific logical interface and enter its configuration mode.

Configuring the Way of Acquiring the IP Address of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the way of acquiring the IP address of the logical interface.

Associating a Dialer Pool

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Associate the logical interface with a specific dialer pool.

Configuring the Encapsulation Protocol

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the encapsulation protocol PPP on the logical interface.

Configuring the MTU of the Logical Interface

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Set the MTU of the logical interface to 1488.

Associating a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Associate a dialer triggering rule.

Configuring the User Name for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name for CHAP authentication.

Configuring the Password for CHAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the password for CHAP authentication.

Configuring the User Name and Password for PAP Authentication

- The configuration is mandatory.
- Perform this configuration in logical interface configuration mode.
- Configure the user name and password for PAP authentication.

Defining a Dialer Triggering Rule

- The configuration is mandatory.
- Perform this configuration in global configuration mode.
- Define a dialer triggering rule.

Verification

- Check whether the dialer interface has acquired an IP address.
- Check whether a correct dialer interface route entry has been established on the device.

Related Commands

Enabling the PPPoE Client Function

Command Syntax	**pppoe enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration	The interface on which the PPPoE client will be enabled must be a WAN Ethernet interface.

Usage	

Binding a Logical Dialer Pool and Specifying the Dialing Mode

Command Syntax	**pppoe-client dial-pool-number** *number* { **dial-on-demand** | **no-ddr**
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	The PPPoE client function must be enabled on the interface first.

Adding a Specific Logical Interface and Entering its Configuration Mode

Command Syntax	**interface dialer** *dialer-number*
Parameter Description	*dialer-number*: interface number
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring the Way of Acquiring the IP Address of the Logical Interface

Command Syntax	**ip address** { **negotiate** | *ip-addr subnet-mask* }
Parameter Description	*ip-addr*: manually configured IP address *subnet-mask*: manually configured subnet mask
Command Mode	Interface configuration mode
Configuration Usage	If you select **negotiate**, the IP address of the dialer interface will be acquired through negotiation. If you manually specify the IP address of the dialer interface, the peer's consent is required during negotiation for the device to work properly.

Associating a Dialer Pool

Command Syntax	**dialer pool** *number*
Parameter Description	*number*: number of the dialer pool
Command Mode	Interface configuration mode
Configuration Usage	An Ethernet interface will be selected from the dialer pool as the dialer interface to perform dialing.

Configuring the Encapsulation Protocol

Command Syntax	**encapsulation ppp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the MTU of the Logical Interface

Command Syntax	**mtu** *1488*
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	Because Internet access is implemented through the PPPoE protocol, the L2 header of a packet is longer than that of a common Ethernet packet.

Associating a Dialer Triggering Rule

Command Syntax	**dialer-group** *dialer-group-number*
Parameter Description	*dialer-group-number*: number of the dialer triggering rule
Command Mode	Interface configuration mode
Configuration Usage	If the DDR mode is specified, the device will be triggered to perform dialing only when a packet meeting the rule is routed to the dialer interface. If the no-DDR mode is specified, the configuration will not take effect on the device.

Configuring the User Name for CHAP Authentication

Command Syntax	**ppp chap hostname** *username*
Parameter Description	*username*: user name
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the Password for CHAP Authentication

Command Syntax	**ppp chap password** *password*
Parameter Descr	*password*: password

iption	
Command Mode	Interface configuration mode
Configuration Usage	N/A

Configuring the User Name and Password for PAP Authentication

Command Syntax	**ppp pap sent-username** *username* **password** *password*
Parameter Description	*username*: user name *password*: password
Command Mode	Interface configuration mode
Configuration Usage	N/A

Defining a Dialer Triggering Rule

Command Syntax	**dialer-list number protocol** *protocol-name* **ip**{ **permit** | **deny** | **list** *access-list-number* }
Parameter Description	*protocol-name*: protocol name *access-list-number*: ACL number
Command Mode	Global configuration mode
Configuration Usage	N/A

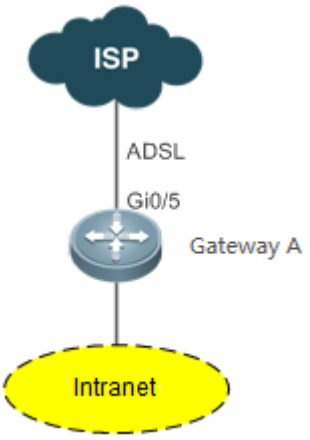
Configuration Example

The following configuration example describes configuration related to the PPPoE client only.

In the ADSL scenario, enable the PPPoE client function and access the Internet through an ADSL line.

Scenario

Figure 8-2



Configuration Steps	● Enable the PPPoE client function on the device, and add the interface Gi0/5 to the dialer pool.
A	A# configure terminal A(config)# interface GigabitEthernet 0/5 A(config-if)# pppoe enable A(config-if)# pppoe-client dial-pool-number 1 no-ddr dial-on-demand A(config-if)# exit A(config)# interface dialer 1 A(config-if)# ip address negotiate A(config-if)# mtu 1488 A(config-if)# encapsulation ppp A(config-if)# ip nat outside A(config-if)# dialer pool 1 A(config-if)# dialer-group 1 A(config-if)# ppp chap hostname pppoe A(config-if)# ppp chap password pppoe A(config-if)# ppp pap sent-username pppoe password pppoe A(config-if)# exit A(config)# access-list 1 permit any A(config)# dialer-list 1 protocol ip permit A(config)# ip nat inside source list 1 interface dialer 1 A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1 A(config)# end A#
Verification	Run the **show ip interface brief | in dialer** *1* command to check whether the dialer interface has acquired an IP address. Run the **show ip route** command to check whether a correct dialer interface route entry has been

	established. A# show ip interface brief | in dialer 1 dialer 1 49.1.1.127/32 YES UP A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is 0.0.0.0 to network 0.0.0.0 S* 0.0.0.0/0 is directly connected, dialer 1 C 10.10.3.0/24 is directly connected, GigabitEthernet 0/0 C 10.10.3.1/32 is local host. C 10.202.172.1/32 is directly connected, dialer 1 C 49.1.1.127/32 is local host.

Common Errors

- The negotiation fails because the user name or password is incorrect.
- Intranet hosts cannot access the Internet because NAT configuration is incorrect.
- Intranet hosts cannot access the Internet because route configuration is incorrect.

8.5 Monitoring

Clearing Various Information

If you run the **clear pppoe tunnel** command while the device is operating, packet forwarding will be interrupted due to tunnel clearance.

Function	Command
Clears statistics about the DDR dialer interface.	**clear dialer** [*interface-type interface-number*]
Clears the tunnel.	**clear pppoe tunnel**

Displaying the Running Status

Function	Command

Displays information about the DDR dialer.	**show dialer** [**interface** type number] [**maps**] [**pools**]
Displays PPPoE status information.	**show pppoe** { **ref** | **session** | **tunnel** }

Displaying Debugging Information

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Command	Function
debug dialer { **pkt** | **mlp|callback|event** }	Enables the DDR debugging switch.
debug ppp [**authentication** | **error** | **event** | **negotiation** | **packet**]	Enables the PPP negotiation debugging switch.
debug pppoe [**datas** | **errors** | **events** | **packets**]	Enables the PPPoE negotiation debugging switch.

9 Configuring RLDP

9.1 Overview

The Rapid Link Detection Protocol (RLDP) achieves rapid detection of unidirectional link failures, directional forwarding failures and downlink loop failures of an Ethernet. When a failure is found, relevant ports will be closed automatically according to failure treatment configuration or the user will be notified to manually close the ports to avoid wrong flow forwarding or an Ethernet layer-2 loop.

9.2 Applications

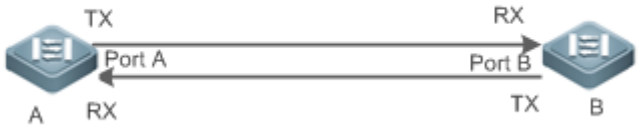
Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

9.2.1 Unidirectional Link Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber. The two lines are the Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If any of the Tx of Port A, Rx of Port B, Tx of Port B and Rx of Port A fails, a unidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 9-1



Remarks	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

- Global RLDP is enabled.
- Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

9.2.2 Bidirectional Forwarding Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber, and the two lines are Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If the Tx of Port A, Rx of Port B, Rx of Port A and Tx of Port B all fail, a bidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 9-2

Remarks	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

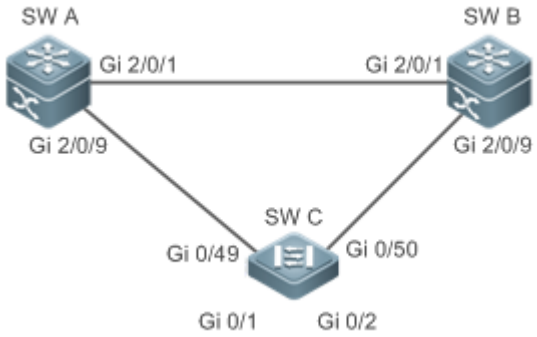
- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

9.2.3 Downlink Loop Detection

Scenario

As shown in the following figure, A, B and C are connect into a loop. Downlink loop detection is enabled on A, and a loop is detected and treated.

Figure 9-3



Remarks	A, B and C are layer-2 or layer-3 switches. A, B and C are interconnected via exchange ports.

Deployment

- Global RLDP is enabled on A.
- Configure downlink loop detection on the Gi 2/0/1 and Gi 2/0/9 ports of A, and define a method for failure treatment.

9.3 Features

Most Ethernet link detection mechanisms detect link connectivity through automatic physical-layer negotiation. However, in some cases devices are connected on the physical layer and operate normally but layer-2 link communication is disabled or abnormal. The RLDP recognizes a neighbor device and detects a link failure through exchanging Prob packets, Echo packets or Loop packets with the device.

Basic Concepts

Unidirectional Link Failure

A unidirectional link failure occurs in case of a cross-connected optical fiber, a disconnected optical fiber, an open-circuit optical fiber, one open-circuit line in a twisted-pair cable, or unidirectional open circuit of an intermediate device between two devices. In such cases, one end of a link is connected and the other disconnected so that flow is forwarded wrongly or a loop guard protocol (for example, the STP) fails.

Bidirectional Link Failure

A bidirectional link failure occurs in case of two optical fibers, two open-circuit lines in a twisted-pair cable, or bidirectional open circuit of an intermediate device between two devices. In such cases, the both ends of a link are disconnected so that flow is forwarded wrongly.

Loop Failure

A downlink device is wrongly connected to form a loop, resulting in a broadcast storm.

RLDP Packet

The RLDP defines three types of packets: Prob packets, Echo packets and Loop packets.

- Prob packets are layer-2 multicast packets for neighbor negotiation, and unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Echo packets are layer-2 unicast packets as response to Prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.
- Loop packets are layer-2 multicast packets for downlink loop detection. They can only be received. The default encapsulation format is SNAP.

RLDP Detection Interval and Maximum Detection Times

A detection interval and the maximum detection times can be configured for the RLDP. A detection interval determines the period of sending Prob packets and Loop packets. When a device receives a Prob packet, it replies with an Echo packet immediately. A detection interval and the maximum detection times determine the maximum detection time (equal to a detection interval × the maximum detection times + 1) for unidirectional or bidirectional link detection. If neither Prob nor Echo packet from a neighbor can be received within the maximum detection time, the treatment of unidirectional or bidirectional failure will be triggered.

RLDP Neighbor Negotiation

When configured with unidirectional or bidirectional link detection, a port can learn a peer-end device as its neighbor. One port may learn one neighbor, which is variable. If negotiation is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation, which succeeds when a port receives a Prob packet from the neighbor. However, if the RLDP is enabled under a failure, the port cannot learn a neighbor so that detection cannot start. In this case, recover the link state before enabling the RLDP.

Treatment for Failed Port under RLDP

- Warning: Only print Syslog to indicate a failed port and a failure type.
- Shutdown SVI: Print Syslog, and then inquire an SVI according to the Access VLAN or Native VLAN of a port and shut down the SVI if the port is a physical exchange port or layer-2 AP member port.
- Port violation: Print Syslog, and configure a failed port as in violation state, and the port will enter Linkdown state physically.
- Block: Print Syslog, and configure the forward state of a port as Block, and the port will not forward packets.

Recovery of Failed Port under RLDP

- Manual reset: Manually reset all failed ports to initialized state and restart link detection.
- Manual or automatic errdisable recovery: Recover all failed ports to initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the treatment for failed ports is not specified as port violation, recover ports to initialized state based on Prob packets and restart link detection.

Port State under RLDP

- normal: Indicates the state of a port after link detection is enabled.
- error: Indicates the state of a port after a unidirectional or bidirectional link failure or a loop failure is detected.

Overview

Feature	Description

Deploying RLDP Detection	Enable unidirectional or bidirectional link detection or downlink loop detection for failures and implement treatment.

9.3.1 Deploying RLDP Detection

The RLDP provides unidirectional link detection, bidirectional forwarding detection and downlink loop detection.

Working Principle

Unidirectional Link Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives Prob packets but no Echo packets, or none of them, treatment for a unidirectional failure will be triggered and detection will stop.

Bidirectional Forwarding Detection

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives neither Prob packets nor Echo packets from a neighbor, treatment for a bidirectional failure will be triggered and detection will stop.

Downlink Loop Detection

When this function is enabled, a port sends Loop packets regularly. In the following cases, a loop failure will be triggered after the same port or a different port receives the packets: in one case, the egress and ingress ports are the same routed port or layer-3 AP member port; in another case, the egress and ingress ports are exchange ports or layer-2 AP member ports in a same default VLAN and in Forward state. Treatment for the failure will be implemented and detection will stop.

Related Configuration

- Configuring RLDP Detection

By default, RLDP detection is disabled.

You may run the global command **rldp enable** or the interface command **rldp port** to enable RLDP detection and specify a detection type and treatment.

You may run the **rldp neighbor-negotiation** command to neighbor negotiation, the **rldp detect-interval** to specify a detection interval, the **rldp detect-max** to specify detection times, or the **rldp reset** to recover a failed port.

9.4 Configuration

Configuration	Description and Command	
Configuring Basic RLDP Functions	⚠ (Mandatory) It is used to enable RLDP detection under global configuration mode.	
	rldp enable	Enables global RLDP detection on all ports.

	(Mandatory)It is used to specify under interface configuration mode a detection type and failure treatment for an interface.	
	rldp port	Enables RLDP detection on a port and specifies a detection type and failure treatment.
	(Optional)It is used to configure a detection interval, detection times and neighbor negotiation under global configuration mode.	
	rldp detect-interval	Modifies global RLDP parameters on all ports, such as the detection interval, maximum detection times and neighbor negotiation.
	rldp detect-max	
	rldp neighbor-negotiation	
	(Optional) It is used under privileged mode.	
	rldp reset	Recovers all ports.

9.4.1 Configuring Basic RLDP Functions

Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional forwarding detection, or downlink loop detection to discover failures.

Notes

- Loop detection is effective to all member ports of an AP when configured on one of the ports. Unidirectional link detection and bidirectional forwarding detection are effective only on an AP member port.
- The loop detection on a physical port added to an AP shall be configured the same as that of the other member ports. There are two cases. First, if loop detection is not configured on a newly-added port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. Second, if a newly-added port and the existing member ports have different loop detection configuration, the new port adopts the configuration and detection results of the existing ports.
- When configuring the RLDP on an AP port, you may configure failure treatment only as "shutdown-port", to which other configurations will be modified.
- When "shutdown-port" is configured on a port, RLDP detection cannot be restored in case of a failure. After troubleshooting, you may run the **rldp reset** or **errdisable recovery** command to restore the port and resume detection. For configuration of the **errdisable recovery** command, please refer to the *Configuring Interface.doc*.

Configuration Steps

Enabling RLDP

- Mandatory.
- Enable RLDP detection on all ports under global configuration mode.

Enabling Neighbor Negotiation

- Optional.
- Enable the function under global configuration mode, and port detection will be started under successful neighbor negotiation.

Configuring Detection Interval

- Optional.
- Specify a detection interval under global configuration mode.

Configuring Maximum Detection Times

- Optional.
- Specify the maximum detection times under global configuration mode.

Configuring Detection under Port

- Mandatory.
- Configure unidirectional RLDP detection, bidirectional RLDP detection or downlink loop detection under interface configuration mode, and specify failure treatment.

Restoring All Failed Ports

- Optional.
- Enable this function under privileged mode to restore all failed ports and resume detection.

Verification

- Display the information of global RLDP, port and neighbor.

Related Commands

Enabling Global RLDP Detection

Command	**rldp enable**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Enable global RLDP detection.

Enabling RLDP Detection on Interface

Command	**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }**
Parameter Description	**unidirection-detect**: Indicates unidirectional link detection. **bidirection-detect**: Indicates bidirectional forwarding detection. **loop-detect**: Indicates downlink loop detection. **warning**: Indicate the failure treatment is warning. **shutdown-svi**: Indicate the failure treatment is closing the SVI that the interface is on. **shutdown-port**: Indicates the failure treatment is port violation. **block**: Indicates the failure treatment is disabling learning and forwarding of a port.
Command Mode	Interface configuration mode
Usage Guide	The interfaces include layer-2 switch ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports. Ports on which RLDP is enabled to handle downlink loop failures are random. For example, RLDP downlink loop detection is configured on both downlink ports A and B, and the configured failure handling mode of port A is **warning** while that of port B is **shutdown-port**. When there is a downlink loop between port A and port B, port A may detect the downlink loop failure prior to port B. After port A completes failure handling according to the configuration, it no longer sends packets to detect the downlink loop status. Port B fails to detect the downlink loop failure because it does not receive a loop detection packet from port A, but the downlink loop actually persists. If a detected downlink loop needs to be actually removed in application scenarios, downlink ports in the same loop must be restricted to use a consistent loop failure handling mode and the loop failure handling mode cannot be **warning**.

Modifying Global RLDP Detection Parameters

Command	**rldp** {**detect-interval** *interval* | **detect-max** *num* | **neighbor-negotiation** }
Parameter Description	**detect-interval** *interval*: Indicates a detection interval. **detect-max** *num*: Indicates detection times. **neighbor-negotiation**: Indicates neighbor negotiation.
Command Mode	Global configuration mode
Usage Guide	Modify all RLDP parameters on all ports when necessary.

Recovering Failed Port

Command	**rldp reset**
Parameter Description	N/A
Command	Privileged mode

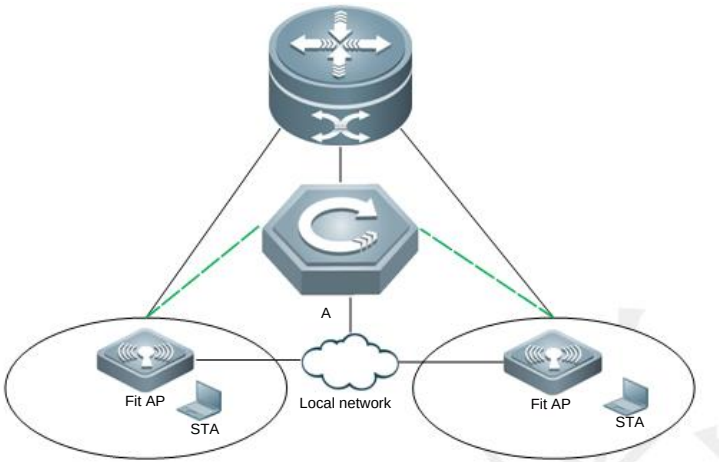
Mode	
Usage Guide	Recover all failed ports to initialized state and resume detection.

Displaying RLDP State Information

Command	**show rldp** [**interface** *interface-name*]
Parameter Description	*interface-name*: Indicates the interface to display information of.
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	Display RLDP state information.

Configuration Example

Configuring RLDP Loop Detection on Wireless APs

Scenario Figure 9-5	As shown in the following figure, a large number of APs exist in the wireless AP scenario. If the RLDP loop detection function is configured and modified on APs one by one, the workload is heavy. The RLDP loop detection configurations can be pushed from the AC device to all online APs (or an independent AP). 
Configuration Steps	● Log in to the AC device and enter the AP configuration mode. ● Enable the RLDP loop detection function on the wired ports of the corresponding AP. ● Enable the RLDP function on corresponding APs in global configuration mode. ● On corresponding APs, configure the recovery time for the RLDP violated port.
A	`A#configure terminal` `A(config)#ap-config all` `A(config-ap)#exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port"` `A(config-ap)#exec-cmd mode configure cmd "rldp enable"` `A(config-ap)#exec-cmd mode configure cmd "errdisable recovery interval 600"`
Verification	● On the AC device, check the RLDP loop detection configurations.

A	`A# show run` `!` `ap-config all` ` exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port"` ` exec-cmd mode configure cmd "rldp enable"` ` exec-cmd mode configure cmd "errdisable recovery interval 600"` `!`

Common Errors

- When the **exec-cmd** command is executed for interface configuration, the input of the corresponding AP wired port is incorrect.
- When the RLDP loop detection configurations are modified, the **no exec-cmd** command is not executed to delete the original configurations or the **exec-cmd** command is not re-executed to cancel the configurations.

9.5 Monitoring

Displaying

Description	Command
Displays RLDP state.	**show rldp** [**interface** *interface-name*]

10 Configuring LLDP

10.1 Overview

The Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is used to discover the topology and identify topological changes. LLDP encapsulates local information of a device into LLDP data units (LLDPDUs) in the type/length/value (TLV) format and then sends the LLDPDUs to neighbors. It also stores LLDPDUs from neighbors in the management information base (MIB) to be accessed by the network management system (NMS).

With LLDP, the NMS can learn about topology, for example, which ports of a device are connected to other devices and whether the rates and duplex modes at both ends of a link are consistent. Administrators can quickly locate and rectify a fault based on the information.

Protocols and Standards

- IEEE 802.1AB 2005: Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices

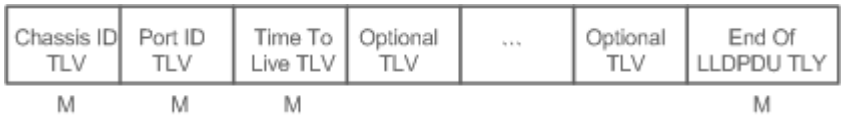
10.2 Features

Basic Concepts

LLDPDU

LLDPDU is a protocol data unit encapsulated into an LLDP packet. Each LLDPDU is a sequence of TLV structures. The TLV collection consists of three mandatory TLVs, a series of optional TLVs, and one End Of TLV. The following figure shows the format of an LLDPDU.

Figure 10-1 LLDPDU Format



In the preceding figure:

- M indicates a mandatory TLV.
- In an LLDPDU, Chassis ID TLV, Port ID TLV, Time To Live TLV, and End Of LLDPDU TLV are mandatory and TLVs of other TLVs are optional.

LLDP Encapsulation Format

LLDP packets can be encapsulated in two formats: Ethernet II and Subnetwork Access Protocols (SNAP).

The following figure shows the format of LLDP packets encapsulated in the Ethernet II format.

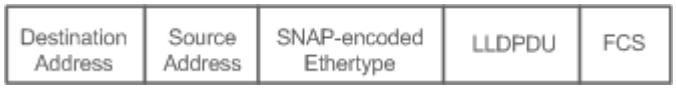
Figure 10-2 Ethernet II Format

In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: Indicates the source MAC address, which is the port MAC address.
- Ethertype: Indicates the Ethernet type, which is 0x88CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

Figure 1-5 shows the format of LLDP packets encapsulated in the SNAP format.

Figure 10-3 SNAP Format



In the preceding figure:

- Destination Address: Indicates the destination MAC address, which is the LLDP multicast address 01-80-C2-00-00-0E.
- Source Address: Indicates the source MAC address, which is the port MAC address.
- SNAP-encoded Ethertype: Indicates the Ethernet type of the SNMP encapsulation, which is AA-AA-03-00-00-00-88-CC.
- LLDPDU: Indicates the LLDP protocol data unit.
- FCS: Indicates the frame check sequence.

TLV

TLVs encapsulated into an LLDPDU can be classified into two types:

- Basic management TLVs
- Organizationally specific TLVs

Basic management TLVs are a collection of basic TLVs used for network management. Organizationally specific TLVs are defined by standard organizations and other institutions, for example, the IEEE 802.1 organization and IEEE 802.3 organization define their own TLV collections.

1. Basic management TLVs

The basic management TLV collection consists of two types of TLVs: mandatory TLVs and optional TLVs. A mandatory TLV must be contained in an LLDPDU for advertisement and an optional TLV is contained selectively.

The following table describes basic management TLVs.

TLV Type	Description	Mandatory/Optional
End Of LLDPDU TLV	Indicates the end of an LLDPDU, occupying two bytes.	Mandatory

Chassis ID TLV	Identifies a device with a MAC address.	Mandatory
Port ID TLV	Identifies a port sending LLDPDUs.	Fixed
Time To Live TLV	Indicates the time to live (TTL) of local information on a neighbor. When a device receives a TLV containing TTL 0, it deletes the neighbor information.	Mandatory
Port Description TLV	Indicates the descriptor of the port sending LLDPDUs.	Optional
System Name TLV	Describes the device name.	Optional
System Description TLV	Indicates the device description, including the hardware version, software version, and operating system information.	Optional
System Capabilities TLV	Describes main functions of the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Indicates the management address, which contains the interface ID and object identifier (OID).	Optional

2. Organizationally specific TLVs

Different organizations, such as the IEEE 802.1, IEEE 802.3, IETF and device suppliers, define specific TLVs to advertise specific information about devices. The organizationally unique identifier (OUI) field in a TLV is used to distinguish different organizations.

- Organizationally specific TLVs are optional and are advertised in an LLDPDU selectively. Currently, there are three types of common organizationally specific TLVs: IEEE 802.1 organizationally specific TLVs, IEEE 802.3 organizationally specific TLVs, and LLDP-MED TLVs.

The following table describes IEEE 802.1 organizationally specific TLVs.

TLV Type	Description
Port VLAN ID TLV	Indicates the VLAN identifier of a port.
Port And Protocol VLAN ID TLV	Indicates the protocol VLAN identifier of a port.
VLAN Name TLV	Indicates the VLAN name of a port.
Protocol Identity TLV	Indicates the protocol type supported by a port.

- IEEE 802.3 organizationally specific TLVs

The following table describes IEEE 802.3 organizationally specific TLVs.

TLV Type	Description
MAC/PHY Configuration//Status TLV	Indicates the rate and duplex mode of a port, and whether to support and enable auto-negotiation.
Power Via MDI TLV	Indicates the power supply capacity of a port.
Link Aggregation TLV	Indicates the link aggregation capacity of a port and the current aggregation state.
Maximum Frame Size TLV	Indicates the maximum size of the frame transmitted by a port.

- LLDP-MED TLV

LLDP-MED is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice Over IP (VoIP) network and detect faults. It provides applications including the network configuration policies, device discovery, PoE management, and inventory management, meeting requirements for low cost, effective management, and easy deployment.

The following table describes LLDP-MED TLVs.

TLV Type	Description
LLDP-MED Capabilities TLV	Indicates the type of the LLDP-MED TLV encapsulated into an LLDPDU and device type (network connectivity device or endpoint device), and whether to support LLDP-MED,.
Network Policy TLV	Advertises the port VLAN configuration, supported application type (such as voice or video services), and Layer-2 priority information.
Location Identification TLV	Locates and identifies an endpoint device.
Extended Power-via-MDI TLV	Provides more advanced power supply management.
Inventory – Hardware Revision TLV	Indicates hardware version of a MED device.
Inventory – Firmware Revision TLV	Indicates the firmware version of the MED device.
Inventory – Software Revision TLV	Indicates the software version of the MED device.
Inventory – Serial Number TLV	Indicates the serial number of the MED device.
Inventory – Manufacturer Name TLV	Indicates the name of the manufacturer of the MED device.
Inventory – Model Name TLV	Indicates the module name of the MED device.
Inventory – Asset ID TLV	Indicates the asset identifier of the MED device, used for inventory management and asset tracking.

Overview

Feature	Description
LLDP Work Mode	Configures the mode of transmitting and receiving LLDP packets.
LLDP Transmission Mechanism	Enables directly connected LLDP-compliant devices to send LLDP packets to the peer.
LLDP Reception Mechanism	Enables directly connected LLDP-compliant devices to receive LLDP packets from the peer.

10.2.1 LLDP Work Mode

Configure the LLDP work mode so as to specify the LLDP packet transmission and reception mode.

Working Principle

LLDP provides three work modes:

- TxRx: Transmits and receives LLDPDUs.
- Rx Only: Only receives LLDPDUs.
- Tx Only: Only transmits LLDPDUs.

When the LLDP work mode is changed, the port initializes the protocol state machine. You can set a port initialization delay to prevent repeated initialization of a port due to frequent changes of the LLDP work mode.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

You can run the **lldp mode** command to configure the LLDP work mode.

If the work mode is set to TxRx, the device can both transmit and receive LLDP packets. If the work mode is set to Rx Only, the device can only receive LLDP packets. If the work mode is set to Tx Only, the device can only transmit LLDP packets. If the work mode is disabled, the device cannot transmit or receive LLDP packets.

10.2.2 LLDP Transmission Mechanism

LLDP packets inform peers of their neighbors. When the LLDP transmission mode is cancelled or disabled, LLDP packets cannot be transmitted to neighbors.

Working Principle

LLDP periodically transmits LLDP packets when working in TxRx or Tx Only mode. When information about the local device changes, LLDP immediately transmits LLDP packets. You can configure a delay time to avoid frequent transmission of LLDP packets caused by frequent changes of local information.
LLDP provides two types of packets:

- Standard LLDP packet, which contains management and configuration information about the local device.
- Shutdown packet: When the LLDP work mode is disabled or the port is shut down, LLDP Shutdown packets will be transmitted. A Shutdown packet consists of the Chassis ID TLV, Port ID TLV, Time To Live TLV, and End OF LLDP TLV. TTL in the Time to Live TLV is 0. When a device receives an LLDP Shutdown packet, it considers that the neighbor information is invalid and immediately deletes it.

When the LLDP work mode is changed from disabled or Rx to TxRx or Tx, or when LLDP discovers a new neighbor (that is, a device receives a new LLDP packet and the neighbor information is not stored locally), the fast transmission mechanism is started so that the neighbor quickly learns the device information. The fast transmission mechanism enables a device to transmit multiple LLDP packets at an interval of 1 second.

Related Configuration

Configuring the LLDP Work Mode

The default work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode tx** command to enable the LLDP packet transmission function. Run the **lldp mode rx** or **no lldp mode** command to disable the LLDP packet transmission function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Rx Only, the device can only receive LLDP packets.

Configuring the LLDP Transmission Delay

The default LLDP transmission delay is 2 seconds.

Run the **lldp timer tx-delay** command to change the LLDP transmission delay.

If the delay is set to a very small value, the frequent change of local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed.

Configuring the LLDP Transmission Interval

The default LLDP transmission interval is 30 seconds.

Run the **lldp timer tx-interval** command to change the LLDP transmission interval.

If the interval is set to a very small value, LLDP packets may be transmitted frequently. If the interval is set to a very large value, the peer may not discover the local device in time.

Configuring the TLVs to Be Advertised

By default, an interface is allowed to advertise TLVs of all types except Location Identification TLV.

Run the **lldp tlv-enable** command to change the TLVs to be advertised.

Configuring the LLDP Fast Transmission Count

By default, three LLDP packets are fast transmitted.

Run the **lldp fast-count** command to change the number of LLDP packets that are fast transmitted.

10.2.3 LLDP Reception Mechanism

A device can discover the neighbor and determine whether to age the neighbor information according to received LLDP packets.

Working Principle

A device can receive LLDP packets when working in TxRx or Rx Only mode. After receiving an LLDP packet, a device conducts validity check. After the packet passes the check, the device checks whether the packet contains information about a new neighbor or about an existing neighbor and stores the neighbor information locally. The device sets the TTL of neighbor information according to the value of TTL TLV in the packet. If the value of TTL TLV is 0, the neighbor information is aged immediately.

Related Configuration

Configuring the LLDP Work Mode

The default LLDP work mode is TxRx.

Run the **lldp mode txrx** or **lldp mode rx** command to enable the LLDP packet reception function. Run the **lldp mode tx** or **no lldp mode** command to disable the LLDP packet reception function.

In order to enable LLDP packet reception, set the work mode to TxRx or Rx Only. If the work mode is set to Tx Only, the device can only transmit LLDP packets.

10.3 Configuration

Configuration	Description and Command	
Configuring the LLDP Function	(Optional) It is used to enable or disable the LLDP function in global or interface configuration mode.	
	lldp enable	Enables the LLDP function.
	no lldp enable	Disables the LLDP function.
Configuring the LLDP Work Mode	(Optional) It is used to configure the LLDP work mode.	
	lldp mode {rx | tx | txrx }	Configures the LLDP work mode.
	no lldp mode	Shuts down the LLDP work mode.
Configuring the TLVs to Be Advertised	(Optional) It is used to configure the TLVs to be advertised.	
	lldp tlv-enable	Configures the TLVs to be advertised.
	no lldp tlv-enable	Cancels TLVs.
Configures the Management Address to Be Advertised	(Optional) It is used to configure the management address to be advertised in LLDP packets.	
	lldp management-address-tlv [*ip-address*]	Configures the management address to be advertised in LLDP packets.
	no lldp management-address-tlv	Cancels the management address.
Configuring the LLDP Fast Transmission Count	(Optional) It is used to configure the number of LLDP packets that are fast transmitted.	
	lldp fast-count *value*	Configures the LLDP fast transmission count.
	no lldp fast-count	Restores the default LLDP fast transmission count.
Configuring the TTL Multiplier and Transmission Interval	(Optional) It is used to configure the TTL multiplier and transmission interval.	
	lldp hold-multiplier *value*	Configures the TTL multiplier.
	no lldp hold-multiplier	Restores the default TTL multiplier.
	lldp timer tx-interval *seconds*	Configures the transmission interval.
	no lldp timer tx-interval	Restores the default transmission interval.
Configuring the Transmission Delay	(Optional) It is used to configure the delay time for LLDP packet transmission.	
	lldp timer tx-delay *seconds*	Configures the transmission delay.
	no lldp timer tx-delay	Restores the default transmission delay.

Configuration	Description and Command	
Configuring the Initialization Delay	(Optional) It is used to configure the delay time for LLDP to initialize on any interface.	
	lldp timer reinit-delay *seconds*	Configures the initialization delay.
	no lldp timer reinit-delay	Restores the default initialization delay.
Configuring the LLDP Trap Function	(Optional) It is used to configure the LLDP Trap function.	
	lldp notification remote-change enable	Enables the LLDP Trap function.
	no lldp notification remote-change enable	Disables the LLDP Trap function.
	lldp timer notification-interval	Configures the LLDP Trap transmission interval.
	no lldp timer notification-interval	Restores the default LLDP Trap transmission interval.
Configuring the LLDP Error Detection Function	(Optional) It is used to configure the LLDP error detection function.	
	lldp error-detect	Enables the LLDP error detection function.
	no lldp error-detect	Disables the LLDP error detection function.
Configuring the LLDP Encapsulation Format	(Optional) It is used to configure the LLDP encapsulation format.	
	lldp encapsulation snap	Sets the LLDP encapsulation format to SNAP.
	no lldp encapsulation snap	Sets the LLDP encapsulation format to Ethernet II.
Configuring the LLDP Network Policy	(Optional) It is used to configure the LLDP Network Policy.	
	lldp network-policy profile *profile-num*	Configures an LLDP Network Policy.
	no lldp network-policy profile *profile-num*	Deletes an LLDP Network Policy.
Configuring the Civic Address	(Optional) It is used to configure the civic address of a device.	
	{ **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*	Configures the civic address of a device.

Configuration	Description and Command	
	no { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*	Deletes civic address of a device.
Configuring the Emergency Telephone Number	⚠ (Optional) It is used to configure the emergency telephone number of a device.	
	lldp location elin identifier *id* **elin-location** *tel-number*	Configures the emergency telephone number of a device.
	no lldp location elin identifier *id*	Deletes the emergency telephone number of a device.

10.3.1 Configuring the LLDP Function

Configuration Effect

- Enable or disable the LLDP function.

Notes

- To make the LLDP function take effect on an interface, you need to enable the LLDP function globally and on the interface.

Configuration Steps

- Optional.
- Configure the LLDP function in global or interface configuration mode.

Verification

Display LLDP status

- Check whether the LLDP function is enabled in global configuration mode.
- Check whether the LLDP function is enabled in interface configuration mode.

Related Commands

↘ Enabling the LLDP Function

Command	**lldp enable**
Parameter De	N/A

scription	
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	The LLDP function takes effect on an interface only after it is enabled in global configuration mode and interface configuration mode.

Disabling the LLDP Function

Command	**no lldp enable**
Parameter De scription	N/A
Command Mode	Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Disabling the LLDP Function

Configuration Steps	Disable the LLDP function in global configuration mode.
	`Ruijie(config)#no lldp enable`
Verification	Display global LLDP status.
	`Ruijie(config)#show lldp status` `Global status of LLDP: Disable`

Common Errors

- If the LLDP function is enabled on an interface but disabled in global configuration mode, the LLDP function does not take effect on the interface.
- A port can learn a maximum of five neighbors.
- If a neighbor does not support LLDP but it is connected to an LLDP-supported device, a port may learn information about the device that is not directly connected to the port because the neighbor may forward LLDP packets.

10.3.2 Configuring the LLDP Work Mode

Configuration Effect

- If you set the LLDP work mode to TxRx, the interface can transmit and receive packets.
- If you set the LLDP work mode to Tx, the interface can only transmit packets but cannot receive packets.
- If you set the LLDP work mode to Rx, the interface can only receive packets but cannot transmit packets.

- If you disable the LLDP work mode, the interface can neither receive nor transmit packets.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Set the LLDP work mode to Tx or Rx as required.

Verification

Display LLDP status information on an interface

Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Work Mode

Command	**lldp mode** { **rx** | **tx** | **txrx** }
Parameter Description	**rx**: Only receives LLDPDUs. **tx**: Only transmits LLDPDUs. **txrx**: Transmits and receives LLDPDUs.
Command Mode	Interface configuration mode
Usage Guide	To make LLDP take effect on an interface, make sure to enable LLDP globally and set the LLDP work mode on the interface to Tx, Rx or TxRx.

Disabling the LLDP Work Mode

Command	**no lldp mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	After the LLDP work mode on an interface is disabled, the interface does not transmit or receive LLDP packets.

Configuration Example

Configuring the LLDP Work Mode

Configuration Steps	Set the LLDP work mode to Tx in interface configuration mode.
	`Ruijie(config)#interface gigabitethernet 0/1`

	Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
Verification	Display LLDP status information on the interface.
	Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : TxOnly Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

10.3.3 Configuring the TLVs to Be Advertised

Configuration Effect

- Configure the type of TLVs to be advertised to specify the LLDPDUs in LLDP packets.

Notes

- If you configure the **all** parameter for the basic management TLVs, IEEE 802.1 organizationally specific TLVs, and IEEE 802.3 organizationally specific TLVs, all optional TLVs of these types are advertised.
- If you configure the **all** parameter for the LLDP-MED TLVs, all LLDP-MED TLVs except Location Identification TLV are advertised.
- If you want to configure the LLDP-MED Capability TLV, configure the LLDP 802.3 MAC/PHY TLV first; If you want to cancel the LLDP 802.3 MAC/PHY TLV, cancel the LLDP-MED Capability TLV first.
- If you want to configure LLDP-MED TLVs, configure the LLDP-MED Capability TLV before configuring other types of LLDP-MED TLVs. If you want to cancel LLDP-MED TLVs, cancel the LLDP-MED Capability TLV before canceling other types of LLDP-MED TLVs If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone.
- If a device supports the DCBX function by default, ports of the device are not allowed to advertise IEEE 802.3 organizationally specific TLVs and LLDP-MED TLVs by default.

Configuration Steps

- Optional.
- Configure the type of TLVs to be advertised on an interface.

Verification

Display the configuration of TLVs to be advertised on an interface

Check whether the configuration takes effect.

Related Commands

Configuring TLVs to Be Advertised

Command	**lldp tlv-enable** { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **|dot1-tlv** { **all | port-vlan-id | protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } **|dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV. **system-description**: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. *vlan-id*: Indicates the Port Protocol VLAN ID, ranging from 1 to 4,094. **vlan-name**: Indicates the VLAN Name TLV. *vlan-id*: Indicates the VLAN name, ranging from 1 to 4,094. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV. **Inventory**: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information. **elin**: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode

Usage Guide	N/A

Canceling TLVs

Command	**no lldp tlv-enable {basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv { all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }
Parameter Description	**basic-tlv**: Indicates the basic management TLV. **port-description**: Indicates the Port Description TLV. **system-capability**: Indicates the System Capabilities TLV. **system-description**: Indicates the System Description TLV. **system-name**: Indicates the System Name TLV. **dot1-tlv**: Indicates the IEEE 802.1 organizationally specific TLVs. **port-vlan-id**: Indicates the Port VLAN ID TLV. **protocol-vlan-id**: Indicates the Port And Protocol VLAN ID TLV. **vlan-name**: Indicates the VLAN Name TLV. **dot3-tlv**: Indicates the IEEE 802.3 organizationally specific TLVs. **link-aggregation**: Indicates the Link Aggregation TLV. **mac-physic**: Indicates the MAC/PHY Configuration/Status TLV. **max-frame-size**: Indicates the Maximum Frame Size TLV. **power**: Indicates the Power Via MDI TLV. **med-tlv**: Indicates the LLDP MED TLV. **capability**: Indicates the LLDP-MED Capabilities TLV. **Inventory**: Indicates the inventory management TLV, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier. **location**: Indicates the Location Identification TLV. **civic-location**: Indicates the civic address information and postal information. **elin**: Indicates the emergency telephone number. *id*: Indicates the policy ID, ranging from 1 to 1,024. **network-policy**: Indicates the Network Policy TLV. *profile-num*: Indicates the Network Policy ID, ranging from 1 to 1,024. **power-over-ethernet**: Indicates the Extended Power-via-MDI TLV.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring TLVs to Be Advertised

Configuration	Cancel the advertisement of the IEEE 802.1 organizationally specific Port And Protocol VLAN ID TLV.

Steps	
	Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Verification	Display LLDP TLV configuration in interface configuration mode.
	Ruijie(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1 LLDP tlv-config of port [GigabitEthernet 0/1] NAME STATUS DEFAULT ------------------------------ ------ ------- Basic optional TLV: Port Description TLV YES YES System Name TLV YES YES System Description TLV YES YES System Capabilities TLV YES YES Management Address TLV YES YES IEEE 802.1 extend TLV: Port VLAN ID TLV YES YES Port And Protocol VLAN ID TLV NO YES VLAN Name TLV YES YES IEEE 802.3 extend TLV: MAC-Physic TLV YES YES Power via MDI TLV YES YES Link Aggregation TLV YES YES Maximum Frame Size TLV YES YES LLDP-MED extend TLV: Capabilities TLV YES YES Network Policy TLV YES YES Location Identification TLV NO NO Extended Power via MDI TLV YES YES

	Inventory TLV YES YES

10.3.4 Configures the Management Address to Be Advertised

Configuration Effect

- Configure the management address to be advertised in LLDP packets in interface configuration mode.
- After the management address to be advertised is cancelled, the management address in LLDP packets is subject to the default settings.

Notes

- LLDP runs on physical ports (AP member ports for AP ports). Stacked ports and VSL ports do not support LLDP.

Configuration Steps

- Optional.
- Configure the management address to be advertised in LLDP packets in interface configuration mode.

Verification

Display LLDP information on a local interface

- Check whether the configuration takes effect.

Related Commands

Configuring the Management Address to Be Advertised

Command	**lldp management-address-tlv** [*ip-address*]
Parameter Description	*ip-address*: Indicates the management address to be advertised in an LLDP packet.
Command Mode	Interface configuration mode
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Canceling the Management Address

Command	**no lldp management-address-tlv**
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	A management address is advertised through LLDP packets by default. The management address is the IPv4 address of the minimum VLAN supported by the port. If no IPv4 address is configured for the VLAN, LLDP keeps searching for the qualified IP address. If no IPv4 address is found, LLDP searches for the IPv6 address of the minimum VLAN supported by the port. If no IPv6 address is found, the loopback address 127.0.0.1 is used as the management address.

Configuration Example

Configuring the Management Address to Be Advertised

Configuration Steps	Set the management address to 192.168.1.1 on an interface.
	Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
Verification	Display configuration on the interface.
	Ruijie(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1 Lldp local-information of port [GigabitEthernet 0/1] Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : GigabitEthernet 0/1 Management address subtype : ipv4 Management address : 192.168.1.1 Interface numbering subtype : ifIndex Interface number : 1 Object identifier : 802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 PPVID Supported : YES PPVID Enabled : NO VLAN name of VLAN 1 : VLAN0001

```
  Protocol Identity                :


  802.3 organizationally information
  Auto-negotiation supported       : YES
  Auto-negotiation enabled         : YES
  PMD auto-negotiation advertised  : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type             : speed(100)/duplex(Full)
  PoE support                      : NO
  Link aggregation supported       : YES
  Link aggregation enabled         : NO
  Aggregation port ID              : 0
  Maximum frame Size               : 1500


  LLDP-MED organizationally information
  Power-via-MDI device type        : PD
  Power-via-MDI power source       : Local
  Power-via-MDI power priority     :
  Power-via-MDI power value        :
  Model name                       : Model name
```

10.3.5 Configuring the LLDP Fast Transmission Count

Configuration Effect

- Configure the number of LLDP packets that are fast transmitted.

Configuration Steps

- Optional.
- Configure the number of LLDP packets that are fast transmitted in global configuration mode.

Verification

Displaying the global LLDP status information

- Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Fast Transmission Count

Command	**lldp fast-count** *value*
Parameter Description	*value*: Indicates the number of LLDP packets that are fast transmitted. The value ranges from 1 to 10. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default LLDP Fast Transmission Count

Command	**no lldp fast-count**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the LLDP Fast Transmission Count

Configuration Steps	Set the LLDP fast transmission count to 5 in global configuration mode.
	`Ruijie(config)#lldp fast-count 5`
Verification	Display the global LLDP status information.
	`Ruijie(config)#show lldp status` `Global status of LLDP : Enable` `Neighbor information last changed time :` `Transmit interval : 30s` `Hold multiplier : 4` `Reinit delay : 2s` `Transmit delay : 2s` `Notification interval : 5s` `Fast start counts : 5`

10.3.6 Configuring the TTL Multiplier and Transmission Interval

Configuration Effect

- Configure the TTL multiplier.
- Configure the LLDP packet transmission interval.

Notes

- Indicates the LLDP packet transmission interval. The value ranges from 1 to 32,768, which is larger than the standard MIB range (5 to 32,768). Thus, it can meet more requirements.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Display LLDP status information on an interface

Check whether the configuration takes effect.

Related Commands

Configuring the TTL Multiplier

Command	**lldp hold-multiplier** *value*
Parameter Description	*value*: Indicates the TLL multiplier. The value ranges from 2 to 10. The default value is 4.
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet. the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV= TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Restoring the Default TTL Multiplier

Command	**no lldp hold-multiplier**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In an LLDP packet, the value of Time To Live TLV is calculated based on the following formula: Time to Live TLV = TTL multiplier x Packet transmission interval + 1. Therefore, you can modify the Time to Live TLV in LLDP packets by configuring the TTL multiplier.

Configuring the Transmission Interval

Command	**lldp timer tx-interval** *seconds*
Parameter De	*seconds*: Indicates the LLDP packet transmission interval. The value ranges from 1 to 32,768.

scription	
Command Mode	Global configuration mode
Usage Guide	N/A

Restoring the Default Transmission Interval

Command	**no lldp timer tx-interval**
Parameter De scription	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the TTL Multiplier and Transmission Interval

Configuration Steps	Set the TTL multiplier to 3 and the transmission interval to 20 seconds. The TTL of local device information on neighbors is 61 seconds.
	`Ruijie(config)#lldp hold-multiplier 3` `Ruijie(config)#lldp timer tx-interval 20`
Verification	Display the global LLDP status information.
	`Ruijie(config)#lldp hold-multiplier 3` `Ruijie(config)#lldp timer tx-interval 20` `Ruijie(config)#show lldp status` `Global status of LLDP : Enable` `Neighbor information last changed time :` `Transmit interval : 20s` `Hold multiplier : 3` `Reinit delay : 2s` `Transmit delay : 2s` `Notification interval : 5s` `Fast start counts : 3`

10.3.7 Configuring the Transmission Delay

Configuration Effect

- Configure the delay time for LLDP packet transmission.

Configuration Steps

- Optional.
- Perform the configuration in global configuration mode.

Verification

Displaying the global LLDP status information

Check whether the configuration takes effect.

Related Commands

Configuring the Transmission Delay

Command	**lldp timer tx-delay** *seconds*
Parameter Description	*seconds*: Indicates the transmission delay. The value ranges from 1 to 8,192.
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Restoring the Default Transmission Delay

Command	**no lldp timer tx-delay**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. Configure the transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information.

Configuration Example

Configuring the Transmission Delay

Configuration Steps	Set the transmission delay to 3 seconds.
	`Ruijie(config)#lldp timer tx-delay 3`
Verification	Display the global LLDP status information.

```
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 3s
Notification interval                 : 5s
Fast start counts                     : 3
```

10.3.8 Configuring the Initialization Delay

Configuration Effect

- Configure the delay time for LLDP to initialize on any interface.

Configuration Steps

- Optional.
- Configure the delay time for LLDP to initialize on any interface.

Verification

Display the global LLDP status information

Check whether the configuration takes effect.

Related Commands

Configuring the Initialization Delay

Command	**lldp timer reinit-delay** *seconds*
Parameter Description	*seconds*: Indicates the initialization delay . The value ranges from 1 to 10 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Restoring the Default Initialization Delay

Command	**no lldp timer reinit-delay**
Parameter De	N/A

scription	
Command Mode	Global configuration mode
Usage Guide	Configure the initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.

Configuration Example

Configuring the Initialization Delay

Configuration Steps	Set the initialization delay to 3 seconds.
	`Ruijie(config)#lldp timer reinit-delay 3`
Verification	Display the global LLDP status information.
	`Ruijie(config)#show lldp status` `Global status of LLDP : Enable` `Neighbor information last changed time :` `Transmit interval : 30s` `Hold multiplier : 4` `Reinit delay : 3s` `Transmit delay : 2s` `Notification interval : 5s` `Fast start counts : 3`

10.3.9 Configuring the LLDP Trap Function

Configuration Effect

- Configure the interval for transmitting LLDP Trap messages.

Configuration Steps

Enabling the LLDP Trap Function

- Optional.
- Perform the configuration in interface configuration mode.

Configuring the LLDP Trap Transmission Interval

- Optional.
- Perform the configuration in global configuration mode.

Verification

Display LLDP status information

Check whether the LLDP Trap function is enabled.

Check whether the interval configuration takes effect.

Related Commands

Enabling the LLDP Trap Function

Command	**lldp notification remote-change enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance

Disabling the LLDP Trap Function

Command	**no lldp notification remote-change enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP Trap function enables a device to send its local LLDP information (such as neighbor discovery and communication link fault) to the NMS server so that administrators learn about the network performance.

Configuring the LLDP Trap Transmission Interval

Command	**lldp timer notification-interval** *seconds*
Parameter Description	*seconds*: Indicates the interval for transmitting LLDP Trap messages. The value ranges from 5 to 3,600 seconds. The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Restoring the LLDP Trap Transmission Interval

Command	**no lldp timer notification-interval**
Parameter Description	N/A
Command	Global configuration mode

Mode	
Usage Guide	Configure the LLDP Trap transmission interval to prevent frequent transmission of LLDP Trap messages. LLDP changes detected within this interval will be transmitted to the NMS server.

Configuration Example

↘ Enabling the LLDP Trap Function and Configuring the LLDP Trap Transmission Interval

Configuration Steps	Enable the LLDP Trap function and set the LLDP Trap transmission interval to 10 seconds.
	Ruijie(config)#lldp timer notification-interval 10 Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Verification	Display LLDP status information.
	Ruijie(config-if-GigabitEthernet 0/1)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 10s Fast start counts : 3 -- Port [GigabitEthernet 0/1] -- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : YES Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

10.3.10 Configuring the LLDP Error Detection Function

Configuration Effect

- Enable the LLDP error detection function. When LLDP detects an error, the error is logged.
- Configure the LLDP error detection function to detect VLAN configuration at both ends of a link, port status, aggregate port configuration, MTU configuration, and loops.

Notes

N/A

Configuration Steps

- Optional.
- Enable or disable the LLDP error detection function in interface configuration mode.

Verification

Display LLDP status information on an interface

Check whether the configuration takes effect.

Related Commands

Enabling the LLDP Error Detection Function

Command	lldp error-detect
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Disabling the LLDP Error Detection Function

Command	no lldp error-detect
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP error detection function relies on specific TLVs in LLDP packets exchanged between devices at both ends of a link. Therefore, a device needs to advertise correct TLVs to ensure the LLDP error detection function.

Configuration Example

Enabling the LLDP Error Detection Function

Configuration Steps	Enable the LLDP error detection function on interface GigabitEthernet 0/1.
	Ruijie(config)#interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect
Verification	Display LLDP status information on the interface.
	Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

10.3.11 Configuring the LLDP Encapsulation Format

Configuration Effect

- Configure the LLDP encapsulation format.

Configuration Steps

- Optional.
- Configure the LLDP encapsulation format on an interface.

Verification

Display LLDP status information of an interface

Check whether the configuration takes effect.

Related Commands

Setting the LLDP Encapsulation Format to SNAP

Command	**lldp encapsulation snap**
Parameter De	N/A

scription	
Command Mode	Interface configuration mode
Usage Guide	The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Restoring the Default LLDP Encapsulation Format (Ethernet II)

Command	**No lldp encapsulation snap**
Parameter De scription	N/A
Command Mode	Interface configuration mode
Usage Guide	The LLDP encapsulation format configuration on a device and its neighbors must be consistent.

Configuration Example

Setting the LLDP Encapsulation Format to SNAP

Configuration Steps	Set the LLDP encapsulation format to SNAP.
	`Ruijie(config)#interface gigabitethernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap`
Verification	Display LLDP status information on the interface.
	`Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1` `Port [GigabitEthernet 0/1]` `Port status of LLDP : Enable` `Port state : UP` `Port encapsulation : Snap` `Operational mode : RxAndTx` `Notification enable : NO` `Error detect enable : YES` `Number of neighbors : 0` `Number of MED neighbors : 0`

10.3.12 Configuring the LLDP Network Policy

Configuration Effect

- Configure the LLDP Network Policy.
- If a device is connected to an IP-Phone that supports LLDP-MED, you can configure the Network Policy TLV to push policy configuration to the IP-Phone, , which enables the IP-Phone to change the tag and QoS of voice streams. In addition to the LLDP Network Policy, perform the following steps on the device: 1. Enable the Voice VLAN function and add the port connected to the IP-Phone to the Voice VLAN. 2. Configure the port connected to the IP-Phone as a QoS trusted port (the trusted DSCP mode is recommended). 3. If 802.1X authentication is also enabled on the port, configure a secure channel for the packets from the Voice VLAN. If the IP-Phone does not support LLDP-MED, enable the voice VLAN function and add the MAC address of the IP-Phone to the Voice VLAN OUI list manually.
- For the configuration of the QoS trust mode, see *Configuring IP QoS*; for the configuration of the Voice VLAN, see *Configuring Voice VLAN*; for the configuration of the secure channel, see *Configuring ACL*.

Configuration Steps

- Optional.
- Configure the LLDP Network Policy.

Verification

Display the LLDP network policy configuration.

Check whether the configuration takes effect.

Related Commands

Configuring the LLDP Network Policy

Command	**lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: Indicates the ID of an LLDP Network Policy. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Deleting the LLDP Network Policy

Command	**no lldp network-policy profile** *profile-num*
Parameter Description	*profile-num*: Indicates the LLDP Network Policy ID. The value ranges from 1 to 1,024.
Command Mode	Interface configuration mode
Usage Guide	Run this command to enter the LLDP network policy mode after specifying a policy ID. After entering the LLDP network policy mode, run the **{ voice | voice-signaling } vlan** command to configure a specific network policy.

Configuration Example

Configuring the LLDP Network Policy

Configuration Steps	Set the Network Policy TLV to 1 for LLDP packets to be advertised by port GigabitEthernet 0/1 and set the VLAN ID of the Voice application to 3, CoS to 4, and DSCP to 6.
	Ruijie#config Ruijie(config)#lldp network-policy profile 1 Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4 Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6 Ruijie(config-lldp-network-policy)#exit Ruijie(config)# interface gigabitethernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
Verification	Display the LLDP network policy configuration on the local device.
	network-policy information: ------------------------- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6

10.3.13 Configuring the Civic Address

Configuration Effect

- Configure the civic address of a device.

Configuration Steps

- Optional.
- Perform this configuration in LLDP Civic Address configuration mode.

Verification

Display the LLDP civic address of the local device

- Check whether the configuration takes effect.

Related Commands

Configuring the Civic Address of a Device

Command	Configure the LLDP civic address. Use the **no** option to delete the address. { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*
Parameter Description	**country**: Indicates the country code, with two characters. CH indicates China. **state**: Indicates the CA type is 1. **county**: Indicates that the CA type is 2. **city**: Indicates that the CA type is 3. **division**: Indicates that the CA type is 4. **neighborhood**: Indicates that the CA type is 5. **street-group**: Indicates that the CA type is 6. **leading-street-dir**: Indicates that the CA type is 16. **trailing-street-suffix**: Indicates that the CA type is 17. **street-suffix**: Indicates that the CA type is 18. **number**: Indicates that the CA type is 19. **street-number-suffix**: Indicates that the CA type is 20. **landmark**: Indicates that the CA type is 21. **additional-location-information**: Indicates that the CA type is 22. **name**: Indicates that the CA type is 23. **postal-code**: Indicates that the CA type is 24. **building**: Indicates that the CA type is 25. **unit**: Indicates that the CA type is 26. **floor**: Indicates that the CA type is 27. **room**: Indicates that the CA type is 28. **type-of-place**: Indicates that the CA type is 29. **postal-community-name**: Indicates that the CA type is 30. **post-office-box**: Indicates that the CA type is 31. **additional-code**: Indicates that the CA type is 32. *ca-word*: Indicates the address.
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Deleting the Civic Address of a Device

Command	**no** { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** }
Parameter Description	N/A

Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the LLDP civic address.

Configuring the Device Type

Command	**device-type** *device-type*
Parameter Description	*device-type*: Indicates the device type. The value ranges from 0 to 2. The default value is 1. 0 indicates that the device type is DHCP server. 1 indicates that the device type is switch. 2 indicates that the device type is LLDP MED .
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, configure the device type.

Restoring the Device Type

Command	**no device-type**
Parameter Description	N/A
Command Mode	LLDP Civic Address configuration mode
Usage Guide	After entering the LLDP Civic Address configuration mode, restore the default settings.

Configuration Example

Configuring the Civic Address of a Device

Configuration Steps	Set the address of port GigabitEthernet 0/1 as follows: set country to CH, city to Fuzhou, and postal code to 350000.
	`Ruijie#config` `Ruijie(config)#lldp location civic-location identifier 1` `Ruijie(config-lldp-civic)# country CH` `Ruijie(config-lldp-civic)# city Fuzhou` `Ruijie(config-lldp-civic)# postal-code 350000`
Verification	Display the LLDP civic address of port GigabitEthernet 0/1 1.
	`civic location information:` `---------------------------` `Identifier :1` `country :CH`

	device type :1 city :Fuzhou postal-code :350000

10.3.14 Configuring the Emergency Telephone Number

Configuration Effect

- Configure the emergency telephone number of a device.

Configuration Steps

- Optional.
- Perform this configuration in global configuration mode.

Verification

Display the emergency telephone number of the local device

- Check whether the configuration takes effect.

Related Commands

Configuring the Emergency Telephone Number of a Device

Command	**lldp location elin identifier** *id* **elin-location** *tel-number*
Parameter Description	*id*: Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024. *tel-number*: Indicates emergency telephone number, containing 10-25 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the emergency telephone number.

Deleting the Emergency Telephone Number of a Device

Command	**no lldp location elin identifier** *id*
Parameter Description	*id*: Indicates the identifier of an emergency telephone number. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Emergency Telephone Number of a Device

Configuration Steps	Set the emergency telephone number of port GigabitEthernet 0/1 to 085285555556.

	Ruijie#config Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
Verification	Display the emergency telephone number of port GigabitEthernet 0/1.
	elin location information: ------------------------- Identifier :1 elin number :085283671111

10.4 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears LLDP statistics.	**clear lldp statistics** [**interface** *interface-name*]
Clears LLDP neighbor information.	**clear lldp table** [**interface** *interface-name*]

Displaying

Description	Command
Displays LLDP information on the local device, which will be organized as TLVs and sent to neighbors.	**show lldp local-information** [**global** | **interface** interface-name]
Displays the LLDP civic address or emergency telephone number of a local device.	**show lldp location** { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-name* **| static** }
Displays LLDP information on a neighbor.	**show lldp neighbors [interface** *interface-name*] [**detail**]
Displays the LLDP network policy configuration of the local device.	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-name* }
Displays LLDP statistics.	**show lldp statistics** [**global | interface** *interface-name*]
Displays LLDP status information.	**show lldp status** [**interface** *interface-name*]
Displays the configuration of TLVs to be advertised by a port.	**show lldp tlv-config** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs LLDP error processing.	**debug lldp error**
Debugs LLDP event processing.	**debug lldp event**
Debugs LLDP hot backup processing.	**debug lldp ha**
Debugs the LLDP packet reception.	**debug lldp packet**
Debugs the LLDP state machine.	**debug lldp stm**

11 Configuring DLDP

11.1 Overview

The Data Link Detection Protocol (DLDP) is a protocol used to quickly detect faulty Ethernet links.

A typical Ethernet link detection mechanism detects physical link connectivity through autonegotiation at the physical layer. Such a mechanism has limitations when detecting Layer-3 data communication exceptions despite normal physical connections.

DLDP provides reliable Layer-3 link detection information. After detecting a faulty link, DLDP shuts down the logical state of Layer-3 ports to realize fast Layer-3 protocol convergence.

11.2 Applications

Application	Description
Intra-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in the same network segment.
Inter-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in different network segments.

11.2.1 Intra-Network Segment DLDP Detection

Scenario

This section describes the basic DLDP application scenario where the source IP address of the detected port and the detected IP address are in the same network segment.

In Figure 11-1, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/2 Layer-3 port on Switch C are in the same network segment. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/2, enable DLDP on Gi 0/1 or Gi 0/2.

Figure 11-1

Remarks	Device A and Device C are switches. Gi 0/1 and Gi 0/2 are Layer-3 ports in the same network segment. B is a network in the same network segment as Gi 0/1 and Gi 0/2.

Deployment

- Enable DLDP on Gi 0/1 or Gi 0/2.

11.2.2 Inter-Network Segment DLDP Detection

Scenario

This section describes the DLDP application scenario where the source IP address of the detected port and the detected IP address are in different network segments.

In Figure 11-2, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/4 Layer-3 port on Switch D are in different network segments. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/4, enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address (IP address of the Gi 0/2 port on Switch B).

Figure 11-2

Remarks	Device A, Device B, and Device D are switches. Gi 0/1 and Gi 0/4 are Layer-3 ports in different network segments.

Deployment

- Enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address.

11.3 Features

Basic Concepts

DLDP Detection Interval and Retransmission Times

Detection interval: Indicates the interval at which DLDP detection packets (ICMP echo) are transmitted.

Retransmission times: Indicate the maximum times DLDP detection packets can be retransmitted in the case of a DLDP detection failure.

When a network device does not receive a reply packet from the peer end within the period of the detection interval multiplied by the retransmission times, the device determines that a Layer-3 link failure occurs and shuts down the logical state of its Layer-3 port (despite the normal physical link connection). When Layer-3 link connectivity is recovered, the device restores its Layer-3 port to Up logical state.

DLDP Detection Modes

Active mode and passive mode are two DLDP detection modes.

Active mode (default): ICMP detection packets are sent actively.

Passive mode: ICMP detection packets are received passively.

DLDP Next Hop

Next hop: Indicates the next node connected to the detected IP address in inter-network segment DLDP detection.

In some cases, DLDP needs to detect IP reachability in non-directly connected network segments. You need to configure the next-hop IP address for the detected port to allow DLDP to obtain the next-hop MAC address through an ARP packet before sending a correct ICMP packet.

In this situation, you need to avoid the return of the reply packet from another link; otherwise, DLDP will misjudge that the detected port does not receive an ICMP reply.

DLDP Recovery Times

Recovery times: Indicate the times DLDP needs to receive consecutive reply packets (ICMP reply) before it can determine link failure recovery.

In some cases, link detection may be unstable. For example, a link is only intermittently pingable. In this case, DLDP repeatedly changes the link status between Up and Down, which may further destabilize the ring network.

Recovery times indicate the times DLDP needs to receive consecutive reply packets before DLDP can set the link in Down state to Up. The default recovery times are three times, indicating that the link needs to be successfully pinged three times before it is set to Up. The recovery times setting reduces link detection sensitivity but increases stability. Related parameters are adjustable according to the network condition.

DLDP Bound MAC Address

Bound MAC address: Indicates the MAC address bound to the detected IP address.

In a complex network environment, DLDP may obtain an invalid MAC address if the detected link has abnormal ARP packets transmitted (causing ARP spoofing), which will make DLDP detection abnormal.

To address this problem, you can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Overview

Feature	Description
DLDP Detection	Detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.
MAC Address Binding	Binds the detected IP address to the MAC address of the detected device to avoid DLDP exceptions otherwise caused by ARP spoofing.
Passive DLDP Detection	When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

11.3.1 DLDP Detection

DLDP detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the corresponding Layer-3 port.

Working Principle

After DLDP detection is enabled, DLDP sends an ARP packet to obtain the MAC address and outbound port of the detected device or the next-hop device. Then DLDP periodically sends IPv4 ICMP echo packets to the MAC address and outbound port to detect link connectivity. If DLDP does not receive an IPv4 ICMP reply packet from the detected device within a specific period, DLDP determines that the link is abnormal and sets the Layer-3 port to Down.

Related Configuration

- Enabling DLDP Detection

By default, DLDP detection is disabled on ports.

Run the **dldp** command with the detected IP address specified to enable DLDP detection.

You can configure the next-hop IP address, MAC address of the detected device, transmission interval, retransmission times, and recovery times based on the actual environment.

11.3.2 MAC Address Binding

The MAC address binding feature is used to bind the detected IP address (or next-hop IP address) to the MAC address of the detected device (or next-hop device) to avoid DLDP exceptions otherwise caused by ARP spoofing

Working Principle

You can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Related Configuration

By default, no MAC address is bound in DLDP detection.

Bind the MAC address of the detected device when you run the **dldp** command to enable DLDP detection. If the next-hop IP address is specified, bind the MAC address of the next-hop device.

After DLDP detection is enabled, DLDP sends ARP packets and ICMP packets with a fixed destination IP address and a fixed destination MAC address. If the source IP address and MAC address in the received packet do not match the bound IP address and MAC address, DLDP will not process the packet.

11.3.3 Passive DLDP Detection

When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

Working Principle

After the device at the local end sends an ICMP echo packet, the peer device determines link connectivity according to the packet reception time by using specific detection parameters, which are the same as those at the local end, thus saving bandwidth and CPU resources.

Related Configuration

By default, passive DLDP detection is disabled.

Run the **dldp passive** command to enable passive DLDP detection.

After passive DLDP detection is enabled, DLDP will return an ICMP reply packet upon receiving an ICMP echo packet, instead of actively sending ICMP echo packets to the peer end. If DLDP does not receive an ICMP echo packet within a specific period, it determines that the link to the peer port is abnormal.

11.4 Configuration

Configuration	Description and Command	
Enabling DLDP Detection	(Mandatory) It is used to enable DLDP detection in interface configuration mode.	
	dldp	Enables DLDP detection.
	(Mandatory) It is used to enable passive DLDP detection in interface configuration mode.	
	dldp passive	Enables passive DLDP detection.
	(Optional) It is used to configure the detection interval, retransmission times, and recovery times of DLDP detection in global configuration mode.	
	dldp interval	Modifies the DLDP parameters globally to apply the modifications to DLDP detection on all ports.
	dldp retry	
	dldp resume	

11.4.1 Enabling DLDP Detection

Configuration Effect

- Detect Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.

Notes

- DLDP supports the configuration of multiple IP addresses on a Layer-3 port. DLDP sets the port to Down when none of the IP addresses receives an ICMP reply. If one IP address resumes communication, DLDP sets the port to Up again.
- DLDP uses the first IP address of the Layer-3 port as the source IP address of detection packets.

Configuration Steps

↘ **Enabling DLDP Detection**

- Mandatory.
- When you enable DLDP detection in interface configuration mode, you can configure the next-hop IP address, MAC address, transmission interval, retransmission times, and recovery times based on the actual environment.

Configuring a DLDP Detection Mode

- Optional.
- You can configure active or passive DLDP detection in interface configuration mode based on the actual environment.
- If DLDP detection needs to be enabled at both ends of a Layer-3 link, you can configure passive DLDP detection at one end to save bandwidth and CPU resources.

Configuring DLDP Parameters Globally

- Optional.
- You can modify the parameters of DLDP detection on all ports in global configuration mode based on requirements. The parameters include the packet transmission interval, packet retransmission times, and recovery times.

Verification

- Display the device DLDP information, including the status and statistics of DLDP detection on all ports.

Related Commands

Enabling DLDP Detection

Command	**dldp** *ip-address* [*next-hop-ip*] [**mac-address** *mac-addr*] [**interval** *tick*] [**retry** *retry-num*] [**resume** *resume-num*]
Parameter Description	*ip-address*: Indicates the detected IP address. *next-hop-ip*: Indicates the next-hop IP address. *mac-addr*: Indicates the MAC address of the detected device to be bound. If the next-hop IP address is specified, bind the MAC address of the next-hop device. *tick*: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s). *retry-num*: The value ranges from 1 to 3,600. The default value is 4. *resume-num*: Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.
Command Mode	Interface configuration mode
Usage Guide	The port to be enabled with DLDP detection must be a Layer-3 port, such as a router port, L3AP port, and SVI port.

Configuring a DLDP Detection Mode

Command	**dldp passive**

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	You need to enable DLDP detection before configuring a DLDP detection mode.

Modifying DLDP Detection Parameters Globally

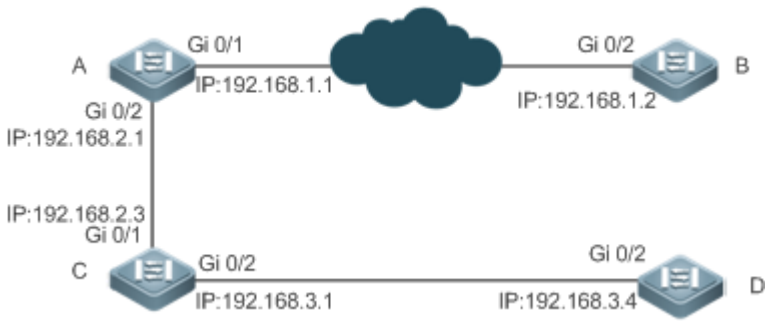
Command	**dldp** { **interval** *tick* | **retry** *retry-num* | **resume** *resume-num* }
Parameter Description	*tick*: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s). *retry-num*: Indicates the interval at which detection packets are retransmitted. The value ranges from 5 to 3,600. The default value is 4. *resume-num:* Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Use this command to quickly modify the parameters of DLDP detection on all ports when the actual environment is changed.

Displaying the DLDP Status

Command	**show dldp statistic** [**interface** *interface-name*]
Parameter Description	*interface-name*: Indicates the Layer-3 port on which the DLDP status will be displayed.
Command Mode	Privileged mode, global configuration mode, and interface configuration mode
Usage Guide	Use this command to display the DLDP status on a specific port. You can also use this command to display the DLDP status on all ports.

Configuration Example

Enabling DLDP Detection on Layer-3 Ports on Device A and Device B in a Layer-3 Network

Scenario Figure 11-3	
	

Verification	● Enable DLDP detection on the Gi 0/1 and Gi 0/2 router ports on Device A to detect the Layer-3 link connectivity between Device A and Device B and that between Device A and Device D. ● To control the Gi 0/2 router port of Device B, enable passive DLDP detection on the port.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#dldp 192.168.1.2 A(config-if-GigabitEthernet 0/1)# exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/1)#dldp 192.168.3.4 192.168.2.3
B	B#configure terminal B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/1)#dldp 192.168.1.1 B(config-if-GigabitEthernet 0/1)#dldp passive
Verification	● Display the DLDP status on Device A and Device B to check whether DLDP detection is enabled and works normally.
A	A# show dldp Interface Type Ip Next-hop Interval Retry Resume State --------- ------- ---------- ---------- -------- ----- ------ ------ Gi0/1 Active 192.168.1.2 100 4 3 Up Gi0/1 Active 192.168.3.4 192.168.2.3 100 4 3 Up
B	B# show dldp Interface Type Ip Next-hop Interval Retry Resume State --------- ------- ---------- ---------- -------- ----- ------ ------ Gi0/2 Passive 192.168.1.1 100 4 3 Up

Common Errors

- An unreachable IPv4 unicast route is misjudged as a DLDP detection failure.
- DLDP detection fails because the peer device does not support ARP/ICMP replies.
- No next-hop IP address is configured in inter-network segment DLDP detection.

11.5 Monitoring

Clearing

Description	Command
Clears DLDP statistics.	**clear dldp** [**interface** *interface-name* [*ip-address*]]

Displaying

Description	Command
Displays the DLDP status.	**show dldp** [**interface** *interface-name*]
Displays the DLDP statistics on the Up/Down port sates.	**show dldp statistic**

IP Address & Application Configuration

1. Configuring IP Addresses and Services
2. Configuring ARP
3. Configuring IPv6
4. Configuring DHCP
5. Configuring DHCPv6
6. Configuring DNS
7. Configuring FTP Server
8. Configuring FTP Client
9. Configuring Tunnel Interfaces
10. Configuring Network Communication Test Tool
11. Configuring TCP
12. Configuring IPv4/IPv6 REF
13. Configuring TFTP
14. Configuring NAT

15. Configuring ARP Proxy

1 Configuring IP Addresses and Services

1.1 Overview

Internet Protocol (IP) sends packets to the destination from the source by using logical (or virtual) addresses, namely IP addresses. At the network layer, routers forward packets based on IP addresses.

Protocols and Standards

- RFC 1918: Address Allocation for Private Internets
- RFC 1166: Internet Numbers

1.2 Applications

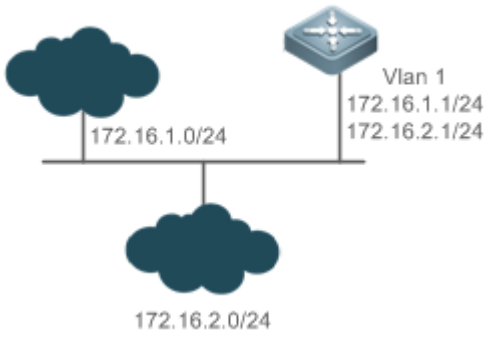
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one switch interface.

1.2.1 Configuring an IP Address for Communication

Scenario

A switch is connected to a Local Area Network (LAN), which is divided into two network segments, namely, 172.16.1.0/24 and 172.16.2.0/24. Computers in the two network segments can communicate with the Internet through switches and computers between the two network segments can communicate with each other.

Figure 1-1Configuring IP Addresses



Deployment

- Configure two IP addresses on VLAN1. One is a primary IP address and the other is a secondary IP address.

- On hosts in the network segment 172.16.1.0/24, set the gateway to 172.16.1.1; on hosts in the network segment 172.16.2.0/24, set the gateway to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal. When expressed in decimal, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by a full stop ".". For example, "192.168.1.1" is an IP address expressed in decimal.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, the network bits and the host bits. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

For a class A address, the most significant bit is 0.7 bits indicate a network ID, and 24 bits indicate a local address. There are 128 class A networks in total.

Figure 1-2

		8	16 24 32
Class A IP address	0	Network ID	Host ID

For a class B address, the first two most significant bits are 10.14 bits indicate a network ID, and 16 bits indicate a local address. There are 16,348 class B networks in total.

Figure 1-3

			8	16 24 32
Class B IP address	1	0	Network ID	Host ID

For a class C address, the first three most significant bits are 110.21 bits indicate a network ID, and 8 bits indicate a local address. There are 2,097,152 class C networks in total.

Figure 1-4

				8	16 24 32
Class C IP address	1	1	0	Network ID	Host ID

For a class D address, the first four most significant bits are 1110 and other bits indicate a multicast address.

Figure 1-5

					8	16	24	32
Class D IP address	1	1	1	0	Multicast address			

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses are called class E addresses and are reserved.

When IP addresses are planned during network construction, IP addresses must be assigned based on the property of the network to be built. If the network needs to be connected to the Internet, users should apply for IP addresses to the corresponding agency. In China, you can apply to China Internet Network Information Center (CNNIC) for IP addresses. Internet Corporation for Assigned Names and Numbers (ICANN) is the final organization responsible for IP address assignment. If the network to be built is an internal private network, users do not need to apply for IP addresses. However, IP addresses cannot be assigned at random. It is recommended to assign dedicated private network addresses.

The following table lists reserved and available addresses.

Class	Address Range	Status
Class A network	0.0.0.0 - 0.255.255.255	Reserved
	1.0.0.0 - 126.255.255.255	Available
	127.0.0.0 - 127.255.255.255	Reserved
Class B network	128.0.0.0 - 191.254.255.255	Available
	191.255.0.0 - 191.255.255.255	Reserved
Class C network	192.0.0.0 - 192.0.0.255	Reserved
	192.0.1.0 - 223.255.254.255	Available
	223.255.255.0 - 223.255.255.255	Reserved
Class D network	224.0.0.0 - 239.255.255.255	Multicast address
Class E network	240.0.0.0 - 255.255.255.254	Reserved
	255.255.255.255	Broadcast address

Three address ranges are dedicated to private networks. These addresses are not used in the Internet. If the networks to which these addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. The following table lists private address ranges. Private network addresses are defined in RFC 1918.

Class	Address Range	Status
Class A network	10.0.0.0 - 10.255.255.255	1 class A network
Class B network	172.16.0.0 - 172.31.255.255	16 class B networks
Class C network	192.168.0.0 - 192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. The bits that identify the IP address are the network address. In a subnet mask, the IP address bits corresponding to the bits whose values are 1s are the network address, and the IP address bits corresponding to the bits whose values are 0s are the host address. For example, for class A networks, the subnet mask is 255.0.0.0. By using network masks, you can divide a network into several subnets. Subnetting means to use some bits of the host address as the network address, thus decreasing the host capacity, and increasing the number of networks. In this case, network masks are called subnet masks.

Broadcast Packet

Broadcast packets refer to the packets destined for all hosts on a physical network. Ruijie products support two types of broadcast packets: (1) directed broadcast, which indicates that all hosts on the specified network are packet receivers and the host bits of a destination address are all 1s; (2) limited broadcast, which indicates that all hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

Internet Control Message Protocol (ICMP) is a sub-protocol in the TCP/IP suite for transmitting control messages between IP hosts and network devices. It is mainly used to notify corresponding devices when the network performance becomes abnormal.

TTL

Time To Live (TTL) refers to the number of network segments where packets are allowed to pass before the packets are discarded. The TTL is a value in an IP packet. It informs the network whether packets should be discarded as the packets stay on the network for a long time.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only after the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured and broadcast packets are forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes are checked.

1.3.1 IP Address

IP addresses are obtained on an interface in the following ways:

1. Manually configuring IP addresses
2. Obtaining IP addresses through DHCP
3. Obtaining IP addresses through PPP negotiation
4. Borrowing IP addresses of other interfaces

These approaches are mutually exclusive. If you configure a new approach to obtain an IP address , the old IP address will be overwritten.

For details on how to obtain IP addresses through DHCP, see the “DHCP” chapter. The following describes the other three approaches for obtaining IP addresses.

Configuring the IP Address for an Interface

A device can receive and send IP packets only after the device is configured with an IP address. Only the interface configured with an IP address can run the IP protocol.

Configuring Multiple IP Addresses for an Interface

Ruijie products support multiple IP address configuration on one interface, of which one is a primary IP address and the others are secondary IP addresses or slave addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, a LAN now needs one class C network to allocate 254 addresses. However, when the number of hosts exceeds 254, one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on L2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, you can connect the isolated subnets by creating a subnet of the isolated network and configuring a secondary address. One subnet cannot be configured on two or more interfaces of a device.

Before configuring secondary IP addresses, make sure that primary IP addresses are configured. If one device in a network is configured with a secondary IP address, other devices must be configured with secondary IP addresses in the same network. If other devices are not configured with IP addresses, the secondary addresses can be set to primary IP addresses.

Obtaining an IP Addresses through PPP Negotiation

This command is supported on point-to-point interfaces only.

Through this configuration, a point-to-point interface accepts the IP address assigned by the peer end through PPP negotiation.

Borrowing an IP Addresses from Another Interface

One interface may not be configured with an IP address. To enable the interface, it must borrow an IP address from another interface.

- IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.
- The IP addresses of borrowed interfaces cannot be borrowed from other interfaces.
- If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.
- The IP address of one interface can be lent to multiple interfaces.
- IP addresses of borrowing interfaces are always consistent with and vary with IP addresses of borrowed interfaces.

Configuring the IP Address of a BVI Interface on an AP through AC

- The configuration modes on an Access Controller (AC) include ap-config apname, ap-group, and ap-config, with priorities in a descending order. The configuration pushed to an Access Point (AP) is the configuration in the highest priority.
- In any AP configuration mode, you can configure an IP address for only one BVI interface by using either the **ap-interface bvi** *num***ip address** *ip-address network-mask* command or the **ap-interface bvi** *num***ip address dynamic** command.
- In a Fit AP network, if the **ap-interface bvi** *num***ip address** *ip-address network-mask* command is used, the AP needs to be assigned within different VLANs. Otherwise, an address conflict occurs. If the **ap-interface bvi** *num***ip address dynamic** command is used, the problem does not occur.

Related Configuration

Configuring an Interface with One or More IP Addresses

- By default, an interface is not configured with an IP address.
- The **ip address** command is used to configure an IP address for an interface.
- After an IP address is configured, the IP address can be used for communication when it passes conflict detection.
- The **ip address** *ip-address mask* **secondary** command can be used to configure multiple secondary IP addresses.

Obtaining an IP Address through PPP Negotiation

- By default, the interface cannot obtain an IP address through PPP negotiation.
- The **ip address negotiate** command is used to configure IP address negotiation on a point-to-point interface.

Borrowing an IP Address from Other Interfaces

- By default, an interface is not configured with an IP address.
- The **ip unnumbered** command can be used to borrow IP addresses from other interfaces.

Configuring the IP Address of a BVI Interface on an AP through AC

- By default, the IP address of a BVI interface is not configured in AP configuration mode.
- The **ap-interface bvi** *num* **ip address** command is used to configure the IP address of a BVI interface of an AP on an AC.

1.3.2 Broadcast Packet Processing

Working Principle

Broadcast is divided into two types. One is limited broadcast, and the IP address is 255.255.255.255. Because the broadcast is prohibited by routers, the broadcast is called local network broadcast. The other is directed broadcast. All host bits are 1s, for example, 192.168.1.255/24. The broadcast packets with these IP addresses can be forwarded.

If IP network devices forward limited broadcast packets (destination IP address is 255.255.255.255), the network may be overloaded, which severely affects network performance. This circumstance is called broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. L2 network devices such as bridges and switches forward and spread broadcast storms.

The best way to avoid broadcast storm is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast rather than limited broadcast to spread data.

For details about broadcast storms, see RFC 919 and RFC 922.

Directed broadcast packets refer to the broadcast packets destined for a subnet. For example, packets whose destination address is 172.16.16.255 are called directed broadcast packets. However, the node that generates the packets is not a member of the destination subnet.

After receiving directed broadcast packets, the devices not directly connected to the destination subnet forward the packets. After directed broadcast packets reach the devices directly connected to the subnet, the devices convert directed broadcast packets to limited broadcast packets (destination IP address is 255.255.255.255) and broadcast the packets to all hosts on the destination subnet at the link layer.

Related Configuration

↘ Configuring an IP Broadcast Address

- By default, the IP broadcast address of an interface is 255.255.255.255.
- To define broadcast packets of other addresses, run the **ip broadcast-address** command on the interface.

↘ Forwarding Directed Broadcast Packets

- By default, directed broadcast packets cannot be forwarded.
- On the specified interface, you can run the **ip directed-broadcast** command to enable directed broadcast packets forwarding. In this way, the interface can forward directed broadcast packets to networks that are directly connected. Broadcast packets can be transmitted within the destination subnet without affecting forwarding of other directed broadcast packets.
- On an interface, you can define an Access Control List (ACL) to transmit certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.3.3 Sending ICMP Packets

Working Principle

ICMP Protocol Unreachable Message

A device receives non-broadcast packets destined for itself, and he packets contain the IP protocol that cannot be processed by the device. The device sends an ICMP protocol unreachable message to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable message.

ICMP Redirection Message

Sometimes, a route may be less than optimal, which makes a device send packets from the interface that receives packets. If a device sends packets from an interface on which it receives the packets, the device sends an ICMP redirection message to the source, informing the source that the gateway is another device on the same subnet. In this way, the source sends subsequent packets according to the optimal path.

ICMP Mask Response Message

Sometimes, a network device sends an ICMP mask request message to obtain the mask of a subnet.. The network device that receives the ICMP mask request message sends a mask response message.

Related Configuration

Enabling ICMP Protocol Unreachable Message

- By default, the ICMP Protocol unreachable message function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling ICMP Redirection Message

- By default, the ICMP redirection message function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling ICMP Mask Response Message

- By default, the ICMP mask response message function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

Enabling Returning of a Timestamp Reply

- By default, returning of a Timestamp Reply is enabled.
- You can run the [**no**] **ip icmp timestamp** command to disable or enable the function.

1.3.4 Limiting Transmission Rate of ICMP Error Packets

Working Principle

This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm.

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively.

Related Configuration

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by DF Bit in the IP Header

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval DF** command can be used to configure the transmission rate.

Configuring the Transmission Rate of Other ICMP Error Packets

- The default transmission rate is 10 packets every 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working Principle

If an IP packet exceeds the IP MTU size, the RGOS software splits the packet. For all devices in the same physical network segment, the IP MTU of interconnected interfaces must be the same. You can adjust the link MTU of interfaces on Ruijie products. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

Related Configuration

Setting the IP MTU

- By default, the IP MTU of an interface is 1500.
- The **ip mtu** command can be used to set the IP packet MTU.

1.3.6 IP TTL

Working Principle

An IP packet is transmitted from the source address to the destination address through routers. After a TTL value is set, the TTL value decreases by 1 every time when the IP packet passes a router. When the TTL value drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 IP Source Route

Working Principle

Ruijie products support IP source routes. When a device receives an IP packet, it checks the options such as source route, loose source route, and record route in the IP packet header. These options are detailed in RFC 791. If the device detects that the packet enables one option, it responds; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the IP source route is enabled, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypasses the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

Related Configuration

↘ **Configuring an IP Source Route**

- By default, the IP source route function is enabled.
- The **ip source-route** command can be used to enable or disable the function.

1.3.8 IP Address Pool

Working Principle

A point-to-point interface can assign an IP address to the peer end through PPP negotiation. During PPP negotiation, the server checks authentication information of the client. If the client passes the authentication, the server assigns an IP address to the client (if the client is configured with an IP address and the IP address meets requirements of the server, the server approves the IP address of the client). The IP address of the peer end can be directly specified or assigned from the address pool.

Related Configuration

↘ **Enabling the Address Pool Function**

- By default, the address pool function is enabled.
- The **ip address-pool local** command can be used to enable or disable the function.

↘ **Creating an Address Pool**

- By default, no IP address pool is configured.
- The **ip local pool** command can be used to create or delete an address pool.

↘ **Assigning an IP Address to the Peer End through PPP Negotiation**

- By default, an interface does not assign an IP address to the peer end.
- The **peer default ip address** command can be used to assign an IP address to the peer end.

1.4 Configuration

Configuration	Description and Command	
Configuring the IP Addresses of an Interface	⚠ (Mandatory) It is used to configure an IP address and allow the IP protocol to run on an interface.	
	ip address	Manually configures the IP address of an interface.
	ip address negotiate	Obtains the IP address of an interface through PPP negotiation.
	ip unnumbered	Borrows an IP address from another interface.
	ap-interface bvi *num* **ip address**	Configures the IP address of a BVI interface on an AP through AC.
Configuring Broadcast Forwarding	⚠ (Optional) It is used to set an IP broadcast address and enable directed broadcast forwarding.	
	ip broadcast-address	Configures an IP broadcast address.
	ip directed-broadcast	Enables directed broadcast forwarding.
Configuring ICMP Forwarding	⚠ (Optional) It is used to enable ICMP packet forwarding.	
	ip unreachables	Enables ICMP unreachable messages and host unreachable messages.
	ip redirects	Enables ICMP redirection messages.
	ip mask-reply	Enables ICMP mask response messages.
	ip icmp timestamp	Enables returning of a Timestamp Reply.
Configuring the Transmission Rate of ICMP Error Packets	⚠ Optional.	
	ip icmp error-interval DF	Configures the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header.
	ip icmp error-interval	Configures the transmission rate of ICMP error packets and ICMP redirection packets.
Setting the IP MTU	⚠ (Optional) It is used to configure the IP MTU on an interface.	
	ip mtu	Sets the MTU value.
Setting the IP TTL	⚠ (Optional) It is used to configure the TTL of unicast packets and broadcast packets.	

Configuration	Description and Command	
	ip ttl	Sets the TTL value.
Configuring an IP Source Route	(Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.

1.4.1 Configuring the IP Addresses of an Interface

Configuration Effect

Configure the IP address of an interface for communication.

Notes

- N/A

Configuration Steps

Configuring the IP Address of an Interface

- Mandatory
- Perform the configuration in L3 interface configuration mode.

Obtaining the IP Address of an Interface through PPP Negotiation

- If a point-to-point interface is not configured with an IP address, obtain an IP address through PPP negotiation.
- Perform the configuration in L3 interface configuration mode.

Borrowing an IP Address from Another Interface

- Optional
- If a point-to-point interface is not configured with an IP address, borrow an IP address from another interface.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Manually Configuring the IP Address of an Interface

Command	**ip address** *ip-address network-mask* [**secondary**]
Parameter Description	*ip-address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. Every 8 bits form one group. The network mask is expressed in decimal and groups are separated by a full stop (.). **secondary**: Secondary IP address.

Command Mode	Interface configuration mode
Usage Guide	N/A

Obtaining an IP Address of an Interface through PPP Negotiation

Command	**ip address negotiate**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Only point-to-point interfaces support obtaining IP addresses through PPP negotiation. After the **ip address negotiate** command is run on an interface, run the **peer default ip address** command at the peer end.

Borrowing an IP Addresses from Another Interface

Command	**ip unnumbered** *interface-type interface-number*
Parameter Description	*interface-type*: Interface type. *interface-number*: Interface ID.
Command Mode	Interface configuration mode
Usage Guide	An unnumbered interface indicates that the interface is enabled with the IP protocol without an IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address. For an IP packet generated on an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface according to its associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations: An Ethernet interface cannot be set to an unnumbered interface. When a serial interface encapsulates SLIP, HDLC, PPP, LAPB, and Frame-Relay, the serial interface can be set to an unnumbered interface. During Frame -Relay encapsulation, however, only a point-to-point interface can be configured as an unnumbered interface. AnX.25 interface cannot be configured as an unnumbered interface. The **ping** command cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface is not configured with an IP address. However, you can monitor the status of an unnumbered interface remotely through SNMP. A device cannot be cold started through an unnumbered interface.

Configuring the IP Address of a BVI Interface on an AP through AC

Command	**ap-interface bvi** *num***ip address** {*ip-address network-mask* | **dynamic**}
Parameter Description	*num*: BVI interface ID. *ip-address*: 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal and groups

	are separated by a full stop (.). *network-mask*: 32-bit network mask. Value 1 indicates the mask bit and 0 indicates the host bit. **dynamic:** Configures the IP address and mask of a BVI interface on an AP by dynamically obtaining IP addresses and masks.
Command Mode	AP configuration mode/AP group configuration mode
Usage Guide	Run the command in AP configuration mode () or AP group configuration mode. In other words, the configuration modes on an AC include ap-config apname, ap-group, and ap-config, with priorities in a descending order. You can configure an IP address for only one BVI interface in any AP configuration mode. According to the priority, the AC selects the configuration of the highest priority and pushes it to the corresponding AP. ⚠ In a Fit AP network, if the **ap-interface bvi** *num***ip address** *ip-address network-mask* command is used, the AP needs to be assigned within different VLANs. Otherwise, an address conflict occurs. If the **ap-interface bvi** *num***ip address dynamic** command is used, the problem does not occur.

Configuration Example

↘ Configuring an IP Address for an Interface

Configuration Steps	Configure IP address 192.168.23.110 255.255.255.0 on interface GigabitEthernet 0/0.
	Ruijie#configure terminal Ruijie(config)#interface gigabitEthernet 0/0 Ruijie(config-if-GigabitEthernet 0/0)# no switchport Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Ruijie# show ip interface gigabitEthernet 0/0 GigabitEthernet 0/0 IP interface state is: UP IP interface type is: BROADCAST IP interface MTU is: 1500 IP address is: 192.168.23.110/24 (primary)

↘ Obtaining the IP Address of an Interface through PPP Negotiation

Configuration Steps	Obtain the IP address of an interface through PPP negotiation.

	Ruijie(config)#int virtual-ppp 1 Ruijie(config-if-Virtual-ppp 1)#ip address negotiate
Verification	Run the **show run** command on the AC to display the configuration.
	Ruijie#show run interface virtual-ppp 1 Building configuration... Current configuration: 48 bytes interface Virtual-ppp 1 ip address negotiate

Configuring the IP Address of a BVI Interface on an AP through AC

Configuration Steps	Configure the IP address of a BVI 2 interface of an AP to 192.168.2.1 255.255.255.0 in ap-config ap120 mode.
	Ruijie(config)#ap-config ap120 You are going to config AP(ap120), which is online now. Ruijie(config-ap)#ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0
Verification	Run the **show ap-config running-config** command on the AC to check whether the configuration takes effect.
	Ruijie# show ap-config running-config ap-config ap120 ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0
	Run the **show ip interface brief** command on the AP to check whether the configuration takes effect.
	Ruijie# show ip interface brief Interface IP-Address(Pri) IP-Address(Sec) Status Protocol BVI 2 192.168.2.1/24 no address up up

1.4.2 Configuring Broadcast Forwarding

Configuration Effect

Set the broadcast address of an interface to 0.0.0.0 and enable directed broadcast forwarding.

Notes

N/A

Configuration Steps

Configuring an IP Broadcast Address

- (Optional) Some old hosts may identify broadcast address 0.0.0.0 only. In this case, set the broadcast address of the target interface to 0.0.0.0.
- Perform the configuration in L3 interface configuration mode.

Enabling Directed Broadcast Forwarding

- (Optional) If you want to enable a host to send broadcast packets to all hosts in a domain that it is not in, enable directed broadcast forwarding.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show running-config interface** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Broadcast Address

Command	**ip broadcast-address** *ip-address*
Parameter Description	*ip-address*: Broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Generally, the destination address of IP broadcast packets is all 1s, which is expressed as 255.255.255.255. The RGOS software can generate broadcast packets of other IP addresses through definition and receive self-defined broadcast packets and the broadcast packets with address 255.255.255.255.

Allowing Forwarding of Directed Broadcast Packets

Command	**ip directed-broadcast** [*access-list-number*]
Parameter Description	*access-list-number*: Access list number, ranging from 1 to 199 and from1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command Mode	Interface configuration mode
Usage Guide	If the **no ip directed-broadcast** command is run on an interface, the RGOS software will discard directed broadcast packets received from the network that is directly connected.

Configuration Example

Configuration Steps	On interface gigabitEthernet 0/1, set the destination address of IP broadcast packets to 0.0.0.0 and enable directed broadcast forwarding. `Ruijie#configure terminal` `Ruijie(config)#interface gigabitEthernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)# no switchport` `Ruijie(config-if-GigabitEthernet 0/1)#ip broadcast-address 0.0.0.0` `Ruijie(config-if-GigabitEthernet 0/1)#ip directed-broadcast`
Verification	Run the **show ip interface** command to check whether the configuration takes effect. `Ruijie#show running-config interface gigabitEthernet 0/1` `ip directed-broadcast` `ip broadcast-address 0.0.0.0`

1.4.3 Configuring ICMP Forwarding

Configuration Effect

Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on an interface.

Notes

N/A

Configuration Steps

Enabling ICMP Unreachable Messages

- By default, ICMP unreachable messages are enabled.
- Optional)The **no ip unreachables** command can be used to disable ICMP unreachable messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Redirection Messages

- By default, ICMP redirection messages are enabled.
- Optional)The **no ip redirects** command can be used to disable ICMP redirection messages.
- Perform the configuration in L3 interface configuration mode.

Enabling ICMP Mask Response Messages

- By default, ICMP mask response messages are enabled.
- Optional)The **no ip mask-reply** command can be used to disable ICMP mask response messages.
- Perform the configuration in L3 interface configuration mode.

Enabling Returning of a Timestamp Reply

- By default, Tmestamp Replies are enabled.
- Optional)The **no ip icmp timestamp** command can be used to disable Temestamp Replies.
- Perform the configuration in global configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

Enabling ICMP Unreachable Messages

Command	**ip unreachables**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Messages

Command	**ip redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Messages

Command	**ip mask-reply**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Disabling Timestamp Replies

Command	**no ip icmp timestamp**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	N/A

Configuration Example

Configuration Steps	Enable ICMP unreachable messages, ICMP redirection messages, and mask response messages on interface gigabitEthernet 0/1.
	Ruijie#configure terminal Ruijie(config)#interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# no switchport Ruijie(config-if-GigabitEthernet 0/1)# ip unreachables Ruijie(config-if-GigabitEthernet 0/1)# ip redirects Ruijie(config-if-GigabitEthernet 0/1)# ip mask-reply
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Ruijie#show ip interface gigabitEthernet 0/1 GigabitEthernet 0/1 ICMP mask reply is: ON Send ICMP redirect is: ON Send ICMP unreachabled is: ON

1.4.4 Configuring the Transmission Rate of ICMP Error Packets

Configuration Effect

Configure the transmission rate of ICMP error packets.

Notes

N/A

Configuration Steps

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

- Optional
- Perform the configuration in global configuration mode.

Configuring the Transmission Rate of Other ICMP Error Packets

- Optional
- Perform the configuration in global configuration mode.

Enabling Returning of a Timestamp Reply

- By default, returning of a Timestamp Reply is enabled.
- You can run the [**no**] **ip icmp timestamp** command to disable or enable the function.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Transmission Rate of ICMP Destination Unreachable Packets Triggered by the DF Bit in the IP Header

Command	**ip icmp error-interval DF** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is from 0 to 2,147,483,647 and the default value is 100 milliseconds. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. If an IP packet needs to be fragmented but the DF bit in the header is set to 1, the device sends an ICMP destination unreachable packet (code 4) to the source host. This ICMP error packet is used to discover the path MTU. When there are too many other ICMP error packets, the ICMP destination unreachable packet (code 4) may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10milliseconds.

Configuring the Transmission Rate of Other ICMP Error Packets

Command	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Refresh cycle of a token bucket. The value range is 0to 2,147,483,647, and the default value is **100** (ms). When the value is **0**, the transmission rate of ICMP error packets is not limited. *bucket-size*: Number of tokens contained in a token bucket. The value range is 1to 200 and the default value is **10**.

Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. It is recommended to set the refresh cycle to integral multiples of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not integral multiples of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to integral multiples of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

Disabling Returning of Timestamp Reply

Command	**no ip icmp timestamp**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the transmission rate of ICMP destination unreachable packets triggered the DF bit in IP header to 100 packets per second and the transmission rate of other ICMP error packets to 10 packets per second.
	`Ruijie(config)# ip icmp error-interval DF 1000 100` `Ruijie(config)# ip icmp error-interval 1000 10`
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	`Ruijie#show running-config | include ip icmp error-interval` `ip icmp error-interval 1000 10` `ip icmp error-interval DF 1000 100`

1.4.5 Setting the IP MTU

Configuration Effect

Adjust the IP packet MTU.

Notes

N/A

Configuration Steps

- (Optional) When the IP MTU of interconnected interfaces is different on devices in the same physical network segment, set the IP MTU to the same value.
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show ip interface** command to check whether the configuration takes effect.

Related Commands

↘ Setting the IP MTU

Command	**ip mtu** *bytes*
Parameter Description	*bytes*: IP packet MTU. The value range is from 68 to 1,500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	Set the IP MTU of interface gigabitEthernet 0/1 to 512 bytes.
	Ruijie#configure terminal Ruijie(config)#interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# no switchport Ruijie(config-if-GigabitEthernet 0/1)#ip mtu 512
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	Ruijie# show ip interface gigabitEthernet 0/1 IP interface MTU is: 512

1.4.6 Setting the IP TTL

Configuration Effect

Modify the IP TTL value of an interface.

Notes

N/A

Configuration Steps

- Optional

- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Setting the IP TTL

Command	**ip ttl** *value*
Parameter Description	*value*: TTL value. The value range is from 0 to 255.
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	• Set the TTL of unicast packets to 100.
	Ruijie#configure terminal Ruijie(config)#ip ttl 100
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Ruijie#show running-config ip ttl 100

1.4.7 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Steps

- By default, the IP source route function is enabled.
- Optional) The **no ip source-route** command can be used to disable the IP source route function.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Configuring an IP Source Route

Command	**ip source-route**
Parameter Description	N/A
Command Mode	Global configuration mode.
Usage Guide	N/A

Configuration Example

Configuration Steps	● Disable the IP source route function.
	`Ruijie#configure terminal` `Ruijie(config)#no ip source-route`
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	`Ruijie#show running-config` `no ip source-route`

1.4.8 Configuring an IP Address Pool

Configuration Effect

Assign an IP address to a client through PPP negotiation.

Notes

N/A

Configuration Steps

Enabling the IP Address Pool Function

- Optional
- Perform the configuration in global configuration mode.

Creating an IP Address Pool

- Optional
- An IP address pool can be created only after the IP address pool function is enabled. After the IP address pool function is disabled, the created address pool is automatically deleted.
- Perform the configuration in global configuration mode.

Assigning an IP Address to the Peer End through PPP Negotiation

- Optional
- Perform the configuration in L3 interface configuration mode.

Verification

Run the **show run-config** command to check whether the configuration takes effect.

Related Commands

Enabling the IP Address Pool Function

Command	**ip address-pool local**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the IP address pool function is enabled. You can configure an IP address pool to assign an IP address to the peer end through PPP negotiation. To disable the IP address pool function, run the **no ip address-pool local** command. All IP address pools configured previously will be deleted.

Creating an IP Address Pool

Command	**ip local pool** *pool-namelow-ip-address*[*high-ip-address*]
Parameter Description	*pool-name*: Name of a local IP address pool. **default** indicates the default address pool name. *low-ip-address*: Smallest IP address in an IP address pool. *high-ip-address*: Optional)Largest IP address in an IP address pool. If the largest IP address is not specified, the IP address pool contains only one IP address, that is, *low-ip-address*.
Command Mode	Global configuration mode
Usage Guide	The command is used to create one or more IP address pools to assign IP addresses to peer ends through PPP negotiation.

Assigning an IP Address to the Peer End through PPP Negotiation

Command	**peer default ip address** {*ip-address* | **pool** [*pool-name*] }
Parameter Description	*ip-address*: IP address assigned to the peer end. *pool-name*: (Optional) Specifies the address pool that assigns IP addresses. If this parameter is not set, IP addresses are assigned from the default address pool.
Command Mode	Interface configuration mode
Usage Guide	If the peer end is not configured with an IP address while the local device is configured with an IP address, you can enable the local device to assign an IP address to the peer end. Run the **ip address negotiate** command on the peer end and the **peer default ip address** command on the local device so that the peer

	end can accept the IP address assigned through PPP negotiation. The **peer default ip address** command can be configured on only PPP or SLIP interfaces. The **peer default ip address pool** command is used to assign an IP address to the peer end from an IP address pool. The IP address pool is configured through the **ip local pool** command. The **peer default ip address** *ip-address* command is used to specify an IP address for the peer end. The command cannot be run on virtual template interfaces or asynchronous interfaces.

Configuration Example

Configuration Steps	● Assign an IP address from address pool “quark” to the peer end on interface “dialer1”.
	Ruijie#configure terminal Ruijie(config)# ip address-pool local Ruijie(config)# ip local pool quark 172.16.23.2 172.16.23.255 Ruijie(config)# interface dialer 1 Ruijie(config-if-dialer 1)#peer default ip address pool quark
Verification	Run the **show run-config** command to check whether the configuration takes effect.
	Ruijie#show running-config ip local pool quark 172.16.23.2 172.16.23.255 ! interface dialer 1 peer default ip address pool quark

1.5 Monitoring

Displaying

Description	Command
Displays the IP address of an interface.	**show ip interface** [*interface-typeinterface-number* | **brief**]
Displays IP packet statistics.	**show ip packet statistics** [**total** | *interface-name*]
Displays address pool statistics.	**show ip pool** [*pool-name*]

2 Configuring ARP

2.1 Overview

In a local area network (LAN), each IP network device has two addresses: 1) local address. Since the local address is contained in the header of the data link layer (DLL) frame, it is a DLL address. However, it is processed by the MAC sublayer at the DLL and thereby is usually called the MAC address. MAC addresses represent IP network devices on LANs. 2) network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

In a LAN, two IP devices can communicate with each other only after they learn the 48-bit MAC address of each other. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution protocols: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. ARP and Proxy ARP are described respectively in RFC 826 and RFC 1027.

ARP is used to bind the MAC address with the IP address. When you enter an IP address, you can learn the corresponding MAC address through ARP. Once the MAC address is obtained, the IP-MAC mapping will be saved to the ARP cache of the network device. With the MAC address, the IP device can encapsulate DLL frames and send them to the LAN. By default, IP and ARP packets on the Ethernet are encapsulated in Ethernet II frames.

Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

2.2 Applications

Application	Description
LAN-based ARP	A user learns the MAC addresses of other users in the same network segment through ARP.
Proxy ARP-based Transparent Transmission	With Proxy ARP, a user can directly communicate with users in another network without knowing that it exists.

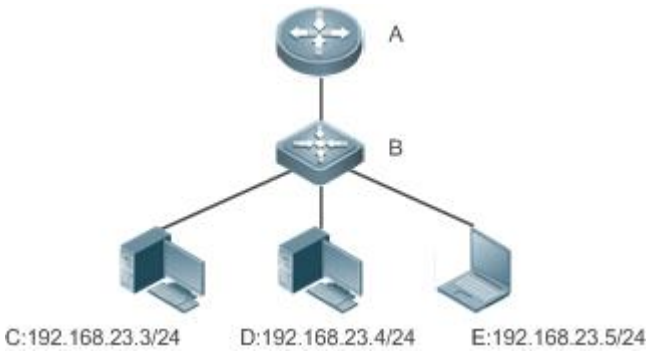
2.2.1 LAN-based ARP

Scenario

ARP is required in all IPv4 LANs.

- A user needs to learn the MAC addresses of other users through ARP to communicate with them.

Figure 2-1



Remarks	A is a router. B is a switch. It acts as the gateway. C, D, and E are hosts.

Deployment

- Enable ARP in a LAN to implement IP-MAC mapping.

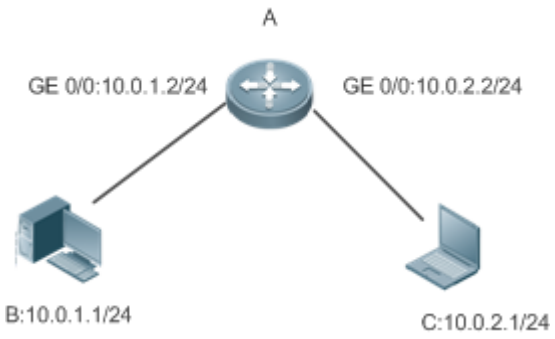
2.2.2 Proxy ARP-based Transparent Transmission

Scenario

Transparent transmission across IPv4 LANs is performed.

- Enable Proxy ARP on the router to achieve direct communication between users in different network segments.

Figure 2-2



Remarks	A is a router connecting two LANs. B and C are hosts in different subnets. No default gateway is configured for them.

Deployment

- Enable Proxy ARP on the subnet gateway. After configuration, the gateway can act as a proxy to enable a host without any route information to obtain MAC addresses of IP users in other subnets.

2.3 Features

Overview

Feature	Description
Static ARP	Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.
ARP Attributes	Users can specify the ARP entry timeout, ARP request retransmission times and interval, and maximum number of unresolved ARP entries.
Trusted ARP	Trusted ARP is used to prevent ARP spoofing.
Gratuitous ARP	Gratuitous ARP is used to detect IP address conflicts and enable peripheral devices to update ARP entries.
Proxy ARP	A proxy replies to the ARP requests from other devices in different subnets.
Local Proxy ARP	A proxy replies to the ARP requests from other devices in the same subnet.
ARP Trustworthiness Detection	Neighbor Unreachable Detection (NUD) is used to ensure that correct ARP entries are learned.
Disabling Dynamic ARP Entry Learning	After dynamic ARP learning is disabled on an interface, the interface does not learn dynamic ARP entries.

2.3.1 Static ARP

Static ARP entries can be configured manually or assigned by the authentication server. The manually configured ones prevail. Static ARP can prevent the device from learning incorrect ARP entries.

Working Principle

If static ARP entries are configured, the device does not actively update ARP entries and these ARP entries permanently exist.

When the device forwards Layer-3 packets, the static MAC address is encapsulated in the Ethernet header as the destination MAC address.

Related Configuration

↘ Enabling Static ARP

Run the **arp** *ip-address mac-address type* command in global configuration mode to configure static ARP entries. By default, no static ARP entry is configured. ARP encapsulation supports only the Ethernet II type, which is represented by ARPA.

2.3.2 ARP Attributes

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Working Principle

ARP Timeout

The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP entry timeout expires, the device sends a unicast ARP request packet to detect whether the peer end is online. If it receives an ARP reply from the peer end, it does not delete this ARP entry. Otherwise, the device deletes this ARP entry.

When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth.

ARP Request Retransmission Interval and Times

The device consecutively sends ARP requests to resolve an IP address to a MAC address. The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request is retransmitted, the more likely the resolution will succeed and the more bandwidth ARP will consume.

Maximum Number of Unresolved ARP Entries

In a LAN, ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the users. To prevent such attacks, users can configure the maximum number of unresolved ARP entries.

Maximum Number of ARP Entries on an Interface

Configure the maximum number of ARP entries on a specified interface to prevent ARP entry resource waste.

Maximum Number of ARP Entries on a Board

Configure the maximum number of ARP entries on a specified slot to limit their ARP capabilities and prevent ARP entry resource waste.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default timeout is 3,600 seconds. You can change it based on actual situations.

Configuring the ARP Request Retransmission Interval and Times

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1 second. You can change it based on actual situations.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission times. The default number of retransmission times is 5. You can change it based on actual situations.

Configuring the Maximum Number of Unresolved ARP Entries

Run the **arp unresolve** *number* command in global configuration mode to configure the maximum number of unresolved ARP entries. The default value is the maximum number of ARP entries supported by the device. You can change it based on actual situations.

Configuring the Maximum Number of ARP Entries on an Interface

Run the **arp cache interface-limit** *limit* command in interface configuration mode to configure the maximum number of ARP entries learned on an interface. The default number is 0. You can change it based on actual situations. This command also applies to static ARP entries.

Configuring the Maximum Number of ARP Entries on a Board

Run the **arp dynamic-entry-limit** *slot-id subslot-id limit* command in global configuration mode to configure the maximum number of ARP entries learned on a specified board. The default number is 0. You can change it based on actual situations.

2.3.3 Trusted ARP

Working Principle

As a type of special ARP entries, trusted ARP entries are added to the ARP table to prevent ARP spoofing. Trusted ARP entries have characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries and lower than that of static ARP entries. Trusted ARP has an aging mechanism similar to that of dynamic ARP. When an ARP entry ages, the device actively sends an ARP request packet to detect whether the corresponding user exists. If the user sends a reply, the device regards the user active and updates the ARP timeout. Otherwise, the device deletes the ARP entry. Trusted ARP has characteristics of static ARP, that is, the device does not learn ARP packets to update the MAC address and interface ID in the ARP entry.

When a user goes online on a GSN client, the authentication server obtains the user's reliable IP-MAC mapping through the access switch, and adds trusted ARP entries to the user's gateway. This process is transparent to the network administrator and does not affect the administrator’s work on network management.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeted at the gateway.

Related Configuration

Enabling Trusted ARP

- Run the **arp trusted user-vlan** *vid1* **translated-vlan** *vid2* command in global configuration mode to implement VLAN redirection. This function is disabled by default. If the VLAN pushed by the server differs from the VLAN in the trusted ARP entry, users need to enable VLAN redirection.
- Run the **arp trusted aging** command in global configuration mode to enable ARP aging. Trusted ARP entries are not aged by default.
- Run the **arp trusted number** command in global configuration mode to configure the capacity of trusted ARP entries. The default value is half of the total capacity of ARP entries. You can change it based on actual situations.

2.3.4 Gratuitous ARP

Working Principle

Gratuitous ARP packets are a special type of ARP packets. In a gratuitous ARP packet, the source and destination IP addresses are the IP address of the local device. Gratuitous ARP packets have two purposes:

5. IP address conflict detection. If the device receives a gratuitous packet and finds the IP address in the packet the same as its own IP address, it sends an ARP reply to notify the peer end of the IP address conflict.
6. ARP update. When the MAC address of an interface changes, the device sends a gratuitous ARP packet to notify other devices to update ARP entries.

The device can learn gratuitous ARP packets. After receiving a gratuitous ARP packet, the device checks whether the corresponding dynamic ARP entry exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

Related Configuration

↘ Enabling Gratuitous ARP

Run the **arp gratuitous-send interval** *seconds* [*number*] command in interface configuration mode to enable gratuitous ARP. This function is disabled on interfaces by default. Generally you need to enable this function on the gateway interface to periodically update the MAC address of the gateway on the downlink devices, which prevents others from faking the gateway.

2.3.5 Proxy ARP

Working Principle

The device enabled with Proxy ARP can help a host without any route information to obtain MAC addresses of IP users in other subnets. For example, if the device receiving an ARP request finds the source IP address in a different network segment from the destination IP address and knows the route to the destination address, the device sends an ARP reply containing its own Ethernet MAC address. This is how Proxy ARP works.

Related Configuration

↘ Enabling Proxy ARP

- Run the **ip proxy-arp** command in interface configuration mode to enable Proxy ARP.
- This function is enabled on routers while disabled on switches by default.

2.3.6 Local Proxy ARP

Working Principle

Local Proxy ARP means that a device acts as a proxy in the local VLAN (common VLAN or sub VLAN).

After local Proxy ARP is enabled, the device can help users to obtain the MAC addresses of other users in the same subnet. For example, when port protection is enabled on the device, users connected to different ports are isolated at Layer 2. After local Proxy ARP is enabled, the device receiving an ARP request acts as a proxy to send an ARP reply containing its own

Ethernet MAC address. In this case, different users communicate with each other through Layer-3 routes. This is how local Proxy ARP works.

Related Configuration

Enabling Local Proxy ARP

- Run the **local-proxy-arp** command in interface configuration mode to enable local Proxy ARP.
- This function is disabled by default.
- This command is supported only on switch virtual interfaces (SVIs).

2.3.7 ARP Trustworthiness Detection

Working Principle

The **arp trust-monitor enable** command is used to enable anti-ARP spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection is enabled on a Layer-3 interface, the device receives ARP request packets from this interface:

1. If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1 to 5 seconds. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry.
2. If the corresponding ARP entry exists, NUD is not performed.
3. If the MAC address in the existing dynamic ARP entry is updated, the device also performs NUD.

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

After this function is disabled, NUD is not required for learning and updating ARP entries.

Related Configuration

Enabling ARP Trustworthiness Detection

Run the **arp trust-monitor enable** command in interface configuration mode to enable ARP trustworthiness detection. This function is disabled by default.

2.3.8 Disabling Dynamic ARP Entry Learning

Working Principle

After dynamic ARP entry learning is disabled on an interface, this interface does not learn dynamic ARP entries.

Related Configuration

Disabling Dynamic ARP Entry Learning

- Dynamic ARP entry learning is enabled on interfaces by default.
- Run the **no arp-learning enable** command in interface configuration mode to disable dynamic ARP entry learning.

2.4 Configuration

Configuration	Description and Command	
Enabling Static ARP	(Optional) It is used to enable static IP-MAC binding.	
	arp	Enables static ARP.
Configuring ARP Attributes	(Optional) It is used to specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the ARP request retransmission interval.
	arp unresolve	Configures the maximum number of unresolved ARP entries.
	arp cache interface-limit	Configures the maximum number of ARP entries on an interface.
Enabling Trusted ARP	(Optional) It is used to enable anti-ARP spoofing.	
	arp trusted user-vlan	Enables VLAN redirection when a trusted ARP entry is added.
	arp trusted aging	Enables trusted ARP aging.
	arp trusted	Configures the capacity of trusted ARP entries.
Enabling Gratuitous ARP	(Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.	
	arp gratuitous-send interval	Enables gratuitous ARP.
Enabling Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from the devices in different subnets.	
	ip proxy-arp	Enables Proxy ARP.
Enabling Local Proxy ARP	(Optional) It is used to act as a proxy to reply to ARP requests from other devices in the same subnet.	
	local-proxy-arp	Enables local Proxy ARP.
Enabling ARP Trustworthiness Detection	(Optional) It is used to unicast ARP request packets to ensure that correct ARP entries are learned.	
	arp trusted-monitor enable	Enables ARP trustworthiness detection.
Disabling Dynamic ARP	(Optional) It is used to disable dynamic ARP learning on an interface.	

Configuration	Description and Command	
Learning	**no arp-learning enable**	Disables dynamic ARP learning on an interface.

2.4.1 Enabling Static ARP

Configuration Effect

Users can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.

Notes

After a static ARP entry is configured, the Layer-3 switch learns the physical port corresponding to the MAC address in the static ARP entry before it performs Layer-3 routing.

Configuration Steps

↘ Configuring Static ARP Entries

- Optional.
- You can configure a static ARP entry to bind the IP address of the uplink device with its MAC address to prevent MAC change caused by ARP attacks.
- Configure static ARP entries in global configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect. Or run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

↘ Configuring Static ARP Entries

Command	**arp** *ip-address mac-address type*
Parameter Description	*ip-address*: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. *mac-address*: Indicates the DLL address, consisting of 48 bits. *type*: Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The RGOS queries a 48-bit MAC address based on a 32-bit IP address in the ARP cache table. Since most hosts support dynamic ARP resolution, usually the static ARP mapping are not configured. Use the **clear arp-cache** command to delete the dynamic ARP entries.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration	Configure a static ARP entry on B to statically bind the IP address of A with the MAC address.

Steps	Ruijie(config)#arp 192.168.23.1 00D0.F822.334B arpa
Verification	Run the **show arp static** command to display the static ARP entry. Ruijie(config)#show arp static Protocol Address Age(min) Hardware Type Interface Internet 192.168.23.1 <static> 00D0.F822.334B arpa 1 static arp entries exist.

Common Errors

- The MAC address in static ARP is incorrect.

2.4.2 Configuring ARP Attributes

Configuration Effect

Users can specify the ARP timeout, ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Configuration Steps

Configuring the ARP Timeout

- Optional.
- In a LAN, if a user goes online/offline frequently, it is recommended to set the ARP timeout small to delete invalid ARP entries as soon as possible.
- Configure the ARP timeout in interface configuration mode.

Configuring the ARP Request Retransmission Interval and Times

- Optional.
- If the network resources are insufficient, it is recommended to set the ARP request retransmission interval great and the retransmission times small to reduce the consumption of network bandwidths.
- Configure the ARP request retransmission interval and times in global configuration mode.

Configuring the Maximum Number of Unresolved ARP Entries

- Optional.
- If the network resources are insufficient, it is recommended to set the maximum number of unresolved ARP entries small to reduce the consumption of network bandwidths.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

Configuring the Maximum Number of ARP Entries on an Interface

- Optional.

- Configure the maximum number of ARP entries on an interface in interface configuration mode.

Configuring the Maximum Number of ARP Entries on a Board

- Optional.
- Configure the maximum number of ARP entries on a board in global configuration mode.

Verification

Run the **show arp timeout** command to display the timeouts of all interfaces.

Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a board.

Related Commands

Configuring the ARP Timeout

Command	**arp timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout in seconds, ranging from 0 to 2,147,483. The default value is 3,600.
Command Mode	Interface configuration mode
Usage Guide	The ARP timeout only applies to the dynamically learned IP-MAC mapping. When the ARP timeout is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. Unless otherwise specified, do not configure the ARP timeout.

Configuring the ARP Request Retransmission Interval and Times

Command	**arp retry interval** *seconds*
Parameter Description	*seconds*: Indicates the ARP request retransmission interval in seconds, ranging from 1 to 3,600. The default value is 1.
Command Mode	Global configuration mode
Usage Guide	If a device frequently sends ARP requests, affecting network performance, you can set the ARP request retransmission interval longer. Ensure that this interval does not exceed the ARP timeout.

Configuring the Maximum Number of Unresolved ARP Entries

Command	**arp unresolve** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ARP entries, ranging from 1 to 8,192. The default value is 8,192.
Command Mode	Global configuration mode
Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, it is recommended to use this command to limit the number of unresolved ARP entries.

Configuring the Maximum Number of ARP Entries on an Interface

Command	**arp cache interface-limit** *limit*
Parameter Description	*limit*: Indicates the maximum number of ARP entries that can be learned on an interface, including configured ARP entries and dynamically learned ARP entries. The value ranges from 0 to the ARP entry capacity supported by the device. 0 indicates no limit on this number.
Command Mode	Interface configuration mode
Usage Guide	Limiting the number of ARP entries on an interface can prevent malicious ARP attacks from generating excessive ARP entries on the device and occupying entry resources. The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	● Set the ARP timeout to 60 seconds on port GigabitEthernet 0/1. ● Set the maximum number of learned ARP entries to 300 on port GigabitEthernet 0/1. ● Set the ARP request retransmission interval to 3 seconds. ● Set the ARP request retransmission times to 4. ● Set the maximum number of unresolved ARP entries to 4,096.
	`Ruijie(config)#interface gigabitEthernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)#arp timeout 60` `Ruijie(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300` `Ruijie(config-if-GigabitEthernet 0/1)#exit` `Ruijie(config)#arp retry interval 3` `Ruijie(config)#arp retry times 4` `Ruijie(config)#arp unresolve 4096`
Verification	● Run the **show arp timeout** command to display the timeout of the interface. ● Run the **show running-config** command to display the ARP request retransmission interval and times, maximum number of unresolved ARP entries, maximum number of ARP entries on the interface, and maximum number of ARP entries on the board.
	`Ruijie#show arp timeout` `Interface arp timeout(sec)` `---------- ----------` `GigabitEthernet 0/1 60` `GigabitEthernet 0/2 3600` `GigabitEthernet 0/4 3600`

```
GigabitEthernet 0/5     3600
GigabitEthernet 0/7     3600
VLAN 100                3600
VLAN 111                3600
Mgmt 0                  3600


Ruijie(config)# show running-config
arp unresolve 4096
arp retry times 4
arp retry interval 3
!
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

2.4.3 Enabling Trusted ARP

Configuration Effect

The gateway is protected from ARP spoofing.

Notes

Configuration Steps

- To deploy a GSN solution, enable trusted ARP.
- To deploy a GSN solution, enable trusted ARP.
- Enable trusted ARP in global configuration mode.

Verification

Run the **show arp trusted** command to display trusted ARP entries.

Run the **show running** command to check whether the configuration takes effect.

Related Commands

↘ **Enabling VLAN Redirection When a Trusted ARP Entry Is Added**

Command	**arp trusted user-vlan** *vid1* **translated-vlan** *vid2*
Parameter	*vid1*: Indicates the VLAN ID configured on the server.

Description	*vid2*: Indicates the ID of the VLAN redirected.
Command Mode	Global configuration mode
Usage Guide	This command takes effect only after trusted ARP is enabled. Configure this command only when the VLAN pushed by the server differs from the VLAN in the trusted ARP entry.

Displaying Trusted ARP Entries

Command	**show arp trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address. The ARP entry of the specified IP address is displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed. *mask*: ARP entries within the IP subnet are displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Deleting Trusted ARP Entries

Command	**clear arp trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address. The ARP entry of the specified IP address is displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed. *mask*: ARP entries within the IP subnet are displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.
Command Mode	Privileged EXEC mode
Usage Guide	After you run the **clear arp trusted** command to delete all trusted ARP entries on the switch, users may fail to access the network. It is recommended to use the **clear arp trusted** *ip* command to delete a specified trusted ARP entry.

Enabling Trusted ARP Aging

Command	**arp trusted aging**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After you configure this command, trusted ARP entries begin to age, with the aging time the same as the dynamic ARP aging time. You can run the **arp timeout** command in interface configuration mode to configure the aging time.

Adjusting the Capacity of Trusted ARP Entries

Command	**arp trusted** *number*

Parameter Description	*number*: The minimum value is 10. The maximum number is the capacity supported by the device minus 1,024. By default, the maximum number of trusted ARP entries is half of the total capacity of ARP entries.
Command Mode	Privileged EXEC mode
Usage Guide	To make this command take effect, enable trusted ARP first. Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the number of ARP entries based on the actual requirement. Do not set it to an excessively large value.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	● Enable VLAN redirection. ● Enable trusted ARP aging. ● Set the maximum number of trusted ARP entries to 1,024.
	Ruijie(config)#arp trusted user-vlan 2-9 translated-vlan 10 Ruijie(config)#arp trusted aging Ruijie(config)#arp trusted 1024
Verification	● Run the **show running-config** command to check whether the configurations take effect.
	Ruijie(config)# show running-config arp trusted user-vlan 2-9 translated-vlan 10 arp trusted aging arp trusted 1024

Common Errors

- Trusted ARP is disabled, causing failure to assign ARP entries.

2.4.4 Enabling Gratuitous ARP

Configuration Effect

The interface periodically sends gratuitous ARP packets.

Configuration Steps

- Optional.
- When a switch acts as the gateway, enable gratuitous ARP on an interface to prevent other users from learning incorrect gateway MAC address in case of ARP spoofing.
- Enable gratuitous ARP in interface configuration mode.

Verification

Run the **show running-config interface** <*name*> command to check whether the configuration is successful.

Related Commands

Enabling Gratuitous ARP

Command	**arp gratuitous-send interval** *seconds* [*number*]
Parameter Description	*seconds*: Indicates the interval for sending a gratuitous ARP request. The unit is second. The value ranges from 1 to 3,600. *number*: Indicates the number of gratuitous ARP requests that are sent. The default value is 1. The value ranges from 1 to 100.
Command Mode	Interface configuration mode
Usage Guide	If a network interface of a device acts as the gateway for downstream devices but a downstream device pretends to be the gateway, enable gratuitous ARP on the interface to advertise itself as the real gateway.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Configure the GigabitEthernet 0/0 interface to send a gratuitous ARP packet every 5 seconds.
	`Ruijie(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5`
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	`Ruijie#sh running-config interface gigabitEthernet 0/0` `Building configuration...` `Current configuration : 127 bytes` `!` `interface GigabitEthernet 0/0` ` duplex auto` ` speed auto` ` ip address 30.1.1.1 255.255.255.0` ` arp gratuitous-send interval 5`

2.4.5 Enabling Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users.

Notes

By default, Proxy ARP is disabled on Layer-3 switches while enabled on routers.

Configuration Steps

- Optional.
- If a user without any route information needs to obtain the MAC addresses of the IP users in other subnets, enable Proxy ARP on the device so that the device can act as a proxy to send ARP replies.
- Enable Proxy ARP in interface configuration mode.

Verification

Run the **show ip interface** <*name*> command to check whether the configuration takes effect.

Related Commands

Enabling Proxy ARP

Command	**ip proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Enable Proxy ARP on port GigabitEthernet 0/0 .
	`Ruijie(config-if-GigabitEthernet 0/0)#ip proxy-arp`
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	`Ruijie#show ip interface gigabitEthernet 0/0` `GigabitEthernet 0/0` `  IP interface state is: DOWN` `  IP interface type is: BROADCAST` `  IP interface MTU is: 1500` `  IP address is:` `    No address configured` `  IP address negotiate is: OFF` `  Forward direct-broadcast is: OFF`

```
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
ARP packet input number: 0
  Request packet     : 0
  Reply packet       : 0
  Unknown packet     : 0
TTL invalid packet number: 0
ICMP packet input number: 0
 Echo request       : 0
 Echo reply         : 0
 Unreachable        : 0
 Source quench      : 0
 Routing redirect   : 0
```

2.4.6 Enabling Local Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users in the same subnet.

Notes

Local Proxy ARP is supported only on SVIs.

Configuration Steps

- Optional.
- If a user enabled with port protection needs to communicate with users in the VLAN, enable local Proxy ARP on the device.
- Enable local Proxy ARP in interface configuration mode.

Verification

Run the **show run interface** <*name*> command to check whether the configuration takes effect.

Related Commands

Enabling Local Proxy ARP

Command	**local-proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Enable local Proxy ARP on the VLAN 1 interface.
	`Ruijie(config-if-VLAN 1)#local-proxy-arp`
Verification	Run the **show ip interface** command to check whether the configuration takes effect.
	`Ruijie#show running-config interface vlan 1` `Building configuration...` `Current configuration : 53 bytes` `interface VLAN 1` ` ip address 192.168.1.2 255.255.255.0` ` local-proxy-arp`

2.4.7 Enabling ARP Trustworthiness Detection

Configuration Effect

Enable ARP trustworthiness detection. If the device receiving an ARP request packet fails to find the corresponding entry, it performs NUD. If the MAC address in the existing dynamic ARP entry is updated, the device immediately performs NUD to prevent ARP attacks.

Notes

Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.

Configuration Steps

- Optional.
- If there is a need for learning ARP entries, enable ARP trustworthiness detection on the device. If the device receiving an ARP request packet fails to find the corresponding entry, it needs to send a unicast ARP request packet to check whether the peer end exists. If yes, the device learns the ARP entry. If not, the device does not learn the ARP entry. If the MAC address in the ARP entry changes, the device will immediately perform NUD to prevent ARP spoofing.
- Enable ARP trustworthiness detection in interface configuration mode.

Verification

Run the **show running-config interface** <*name*> command to check whether the configuration take effect

Related Commands

Enabling ARP Trustworthiness Detection

Command	**arp trust-monitor enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function. If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD. Enable this function. If the MAC address of the existing dynamic ARP entry is updated, the device immediately performs NUD. After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Enable ARP trustworthiness detection on port GigabitEthernet 0/0.
	`Ruijie(config-if-GigabitEthernet 0/0)#arp trust-monitor enable`
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.
	`Ruijie#show running-config interface gigabitEthernet 0/0` `Building configuration...` `Current configuration : 184 bytes` `!` `interface GigabitEthernet 0/0`

	duplex auto speed auto ip address 30.1.1.1 255.255.255.0 arp trust-monitor enable

2.4.8 Disabling Dynamic ARP Learning

Configuration Effect

After dynamic ARP learning is disabled on an interface, the interface does not learn dynamic ARP entries.

Configuration Steps

- Optional.
- Enable dynamic ARP learning in interface configuration mode.

Verification

Run the **show running-config interface** <*name*> command to check whether the configuration takes effect.

Related Commands

Disabling Dynamic ARP Learning

Command	**no arp-learning enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If the device has learned the dynamic ARP entries and converted the ARP entries into static ARP entries through Web, disable dynamic ARP learning. Otherwise, enable dynamic ARP learning. After this function is enabled, users can convert dynamic ARP entries into static ARP entries through Web. Users can also use the **clear arp** command to clear ARP entries to deny a user Internet access. If the **clear arp** command is not configured, dynamic ARP entries will be cleared when the timeout expires. After the dynamic ARP learning function is disabled on an interface, the any IP ARP and ARP trustworthiness detection functions will not work.

Configuration Example

Scenario	For the network topology, see Figure 2-1.
Configuration Steps	Disable dynamic ARP entry learning on port GigabitEthernet 0/0.
	Ruijie(config-if-GigabitEthernet 0/0)#no arp-learning enable
Verification	Run the **show running-config interface** command to check whether the configuration takes effect.

```
Ruijie#sh running-config interface gigabitEthernet 0/0


Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 no arp-learning enable
```

2.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.	**clear arp-cache**

Displaying

Description	Command
Displays the ARP table.	**show ip arp**
Displays the trusted ARP table.	**show arp trusted** [*ip* [*mask*]]
Displays the ARP entry counter.	**show arp counter**
Displays the timeout of dynamic ARP entries.	**show arp timeout**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ARP packet sending and	**debug arp**

receiving.	
Debugs the creation and deletion of ARP entries.	**debug arp event**

3 Configuring IPv6

3.1 Overview

As the Internet develops rapidly and IPv4 address space is becoming exhausted, IPv4 limitations become more and more obvious. At present, many researches and practices on Internet Protocol Next Generation (IPng) have been conducted. The IPng working group of the Internet Engineering Task Force (IETF) has formulated an IPng protocol named IP Version 6 (IPv6), which is described in RFC 2460.

Main Features

Larger Address Space

Compared with 32 bits in an IPv4 address, the length of an IPv6 address is extended to 128 bits. Therefore, the address space has approximately 2^{128} addresses. IPv6 adopts a hierarchical address allocation mode to support address allocation of multiple subnets from the Internet core network to intranet subnet.

Simpler Packet Header Format

Since the design principle of the IPv6 packet header is to minimize the overhead of the packet header, some non-key fields and optional fields are removed from the packet header to the extended packet header. Therefore, although the length of an IPv6 address is four times of that of an IPv4 address, the IPv6 packet header is only two times of the IPv4 packet header. The IPv6 packet header makes device forwarding more efficient. For example, with no checksum in the IPv6 packet header, the IPv6 device does not need to process fragments (fragmentation is completed by the initiator).

Efficient Hierarchical Addressing and Routing Structure

IPv6 uses a convergence mechanism and defines a flexible hierarchical addressing and routing structure. Multiple networks at the same layer are represented as a uniform network prefix on the upstream device, greatly reducing routing entries maintained by the device and routing and storage overheads of the device.

Easy Management: Plug and Play (PnP)

IPv6 provides automatic discovery and auto-configuration functions to simplify management and maintenance of network nodes. For example, Neighbor Discovery (ND), MTU Discovery, Router Advertisement (RA), Router Solicitation (RS), and auto-configuration technologies provide related services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful auto-configuration and stateless auto-configuration. In IPv4, Dynamic Host Configuration Protocol (DHCP) realizes auto-configuration of the host IP address and related parameters. IPv6 inherits this auto-configuration service from IPv4 and called it stateful auto-configuration (see DHCPv6). Besides, IPv6 also offers the stateless auto-configuration service.During stateless auto-configuration, a host automatically obtains the local address of the link, address prefix of the local device, and other related configurations.

Security

As an optional extension protocol of IPv4, Internet Protocol Security (IPSec) is a part of IPv6 to provide security for IPv6 packets. At present, IPv6 provides two mechanisms: Authentication Header (AH) and Encapsulated Security Payload (ESP). AH provides data integrity and authenticates IP packet sources to ensure that the packets originate from the nodes identified by the source addresses. ESP provides data encryption to realize end-to-end encryption.

Better QoS Support

A new field in the IPv6 packet header defines how to identify and process data streams. The Flow Label field in the IPv6 packet header is used to authenticate a data flow. Using this field, IPv6 allows users to propose requirements on the communication quality. , A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

New Protocol for Neighboring Node Interaction

IPv6 Neighbor Discovery Protocol (NDP) uses a series of Internet Control Message Protocol Version 6 (ICMPv6) packets to implement interactive management of neighboring nodes (nodes on the same link). IPv6 uses NDP packets and efficient multicast/unicast ND packets instead of broadcast-based Address Resolution Protocol (ARP) and Control Message Protocol Version 4 (ICMPv4) router discovery packets.

Extensibility

With strong extensibility, IPv6 features can be added to the extended packet header following the IPv6 packet header. Unlike IPv4, the IPv6 packet header can support at most 40 bytes of options. For an IPv6 packet, the length of the extended packet header is restricted only by the maximum number of bytes in the packet.

Protocols and Standards

- RFC 4291 - IP Version 6 Addressing Architecture
- RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 - IPv6 Stateless Address Auto-configuration
- RFC 5059 - Deprecation of Type 0 Routing Headers in IPv6

3.2 Applications

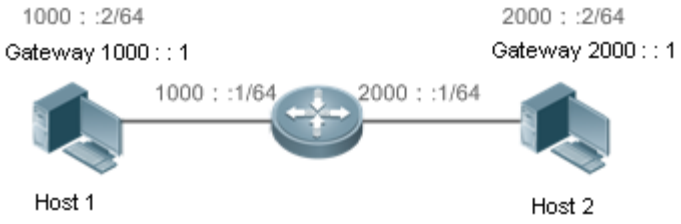
Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

3.2.1 Communication Based on IPv6 Addresses

Scenario

As shown in Figure 3-1, Host 1 and Host 2 communicate with each other using IPv6 addresses.

Figure 3-1



Deployment

Hosts can use the stateless address auto-configuration or DHCPv6 address assignment mode. After addresses are configured, hosts can communicate with each other using IPv6 addresses.

3.3 Features

Overview

Feature	Description
IPv6 Address Format	The IPv6 address format makes IPv6 have a larger address space and flexible representation approach.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies the fixed and extended packet headers to improve the data packet processing and forwarding efficiency of the device.
IPv6 PMTUD	A host dynamically discovers and adjusts the MTU size on the data Tx path, saving router resources and improving IPv6 network efficiency.
IPv6 Neighbor Discovery	ND functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection.
IPv6 Source Routing	This feature is used to specify the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Restricting the Sending Rate of ICMPv6 Error Messages	This feature prevents DoS attacks.
IPv6 HOP-LIMIT	This feature prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.

Feature	Description
Default Gateway on the Management Interface	The default gateway is configured on the management interface to generate a default route for this interface.

3.3.1 IPv6 Address Format

An IPv6 address is represented in the X:X:X:X:X:X:X:X format, where X is a 4-digit hexadecimal integer (16 bits). Each address consists of 8 integers, with a total of 128 bits (each integer contains 4 hexadecimal digits and each digit contains four bits). The following are three valid IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

These integers are hexadecimal, where A to F represent 10 to 15. Each integer in the address must be represented, except the leading zeros in each integer. If an IPv6 address contains a string of zeros (as shown in the second and third examples above), a double colon (::) can be used to represent these zeros. That is, 800:0:0:0:0:0:0:1 can be represented as 800::1.

A double colon indicates that this address can be extended to a complete 128-bit address. In this approach, only when the 16-bit integers are all 0s, can they can be replaced with a double colon. A double colon can exist once in an IPv6 address.

In IPv4/IPv6 mixed environment, an address has a mixed representation. In an IPv6 address, the least significant 32 bits can be used to represent an IPv4 address. This IPv6 address can be represented in a mixed manner, that is, X:X:X:X:X:X:d.d.d.d, where X is a hexadecimal integer and d is a 8-bit decimal integer. For example, 0:0:0:0:0:0:192.168.20.1 is a valid IPv6 address. It can be abbreviated to :::192.168.20.1. Typical applications are IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. If the first 96 bits are 0 in an IPv4-compatible IPv6 address, this address can be represented as ::A.B.C.D, e.g., ::1.1.1.1. IPv4-compatible addresses have been abolished at present. IPv4-mapped IPv6 addresses are represented as ::FFFF:A.B.C.D to represent IPv4 addresses as IPv6 addresses. For example, IPv4 address 1.1.1.1 mapped to an IPv6 address is represented as ::FFFF:1.1.1.1.

Since an IPv6 address is divided into two parts: subnet prefix and interface ID, it can be represented as an address with an additional value according to an address allocation method like Classless Inter-Domain Routing (CIDR). The additional value indicates how many bits (subnet prefix) in the address represent the network part. That is, the IPv6 node address contains the prefix length. The prefix length is separated from the IPv6 address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length used for routing is 60 bits.

Related Configuration

↘ Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure an IPv6 address on an interface.
- After configuration, a host can communicate with others using the configured IPv6 address based on DAD.

3.3.2 IPv6 Address Type

RFC 4291 defines three types of IPv6 addresses:

- Unicast address: ID of a single interface. Packets destined to a unicast address are sent to the interface identified by this address.
- Multicast address: ID of an interface group (the interfaces generally belong to different nodes). Packets destined to a multicast address are sent to all interfaces included in this address.
- Anycast address: ID of an interface group. Packets destined to an anycast address are sent to one interface included in this address (the nearest interface according to the routing protocol).

⚠ IPv6 does not define broadcast addresses.

These three types of addresses are described as follows:

Unicast Addresses

Unicast addresses fall into five types: unspecified address, loopback address, link-local address, site-local address, and global unicast address. At present, site-local addresses have been abolished. Except unspecified, loopback, and link-local addresses, all other addresses are global unicast addresses.

- Unspecified address

The unspecified address is 0:0:0:0:0:0:0:0, which is usually abbreviated to ::. It has two general purposes:

1. If a host has no unicast address when started, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
2. When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts in the same network segment and uses the unspecified address as the source address to send a Neighbor Solicitation (NS) packet (similar to a free ARP packet).

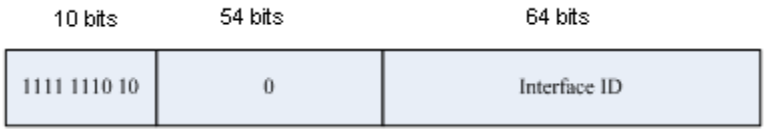
- Loopback address

The loopback address is 0:0:0:0:0:0:0:1, which is usually abbreviated to ::1. Similar to IPv4 address 127.0.0.1, the loopback address is generally used by a node to send itself packets.

- Link-local address

The format of a link-local address is as follows:

Figure 3-2

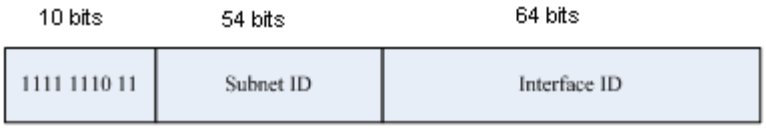


The link-local address is used on a single network link to assign IDs to hosts. The address identified by the first 10 bits in the prefix is the link-local address. A device never forwards packets in which the source or destination address contains the link-local address. The intermediate 54 bits in the address are all 0s. The last 64 bits represent the interface ID, which allows a single network to connect 2^{64}-1 hosts.

- Site-local address

The format of a site-local address is as follows:

Figure 3-3

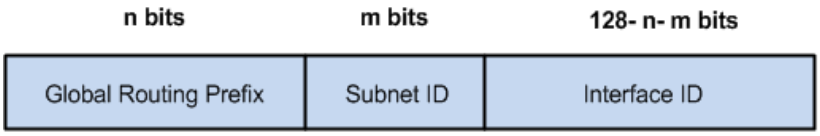


A site-local address is used to transmit data within a site. A device never forwards packets in which the source or destination address contains the site-local address to the Internet. That is, these packets can be forwarded only within the site. A site can be assumed as an enterprise's local area network (LAN). Such addresses are similar to IPv4 private addresses such as 192.168.0.0/16. RFC 3879 has abolished site-local addresses. New addresses do not support the first 10 bits as the prefix and are all regarded as global unicast addresses. Existing addresses can continue to use this prefix.

- Global unicast address

The format of a global unicast address is as follows:

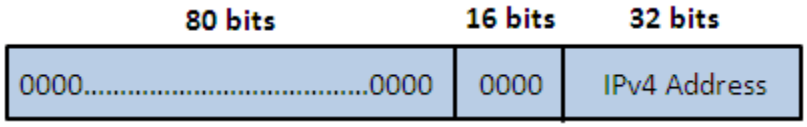
Figure 3-4



Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 nodes and IPv6 nodes.

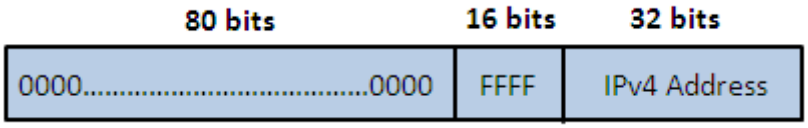
The format of an IPv4-compatible IPv6 address is as follows:

Figure 3-5



The format of an IPv4-mapped IPv6 address is as follows:

Figure 3-6



IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. At present, IPv4-compatible IPv6 addresses have been abolished. IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if the

IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

↘ Multicast Addresses

The format of an IPv6 multicast address is as follows:

```
|    8     |  4 |  4 |                   112 bits                   |
+--------+----+----+----------------------------------------------+
|11111111|flgs|scop|                    group ID                    |
+--------+----+----+----------------------------------------------+
```

The first byte in the address is all 1s, representing a multicast address.

- Flag field

The flag field consists of four bits. Currently only the fourth bit is specified to indicate whether this address is a known multicast address assigned by the Internet Assigned Numbers Authority (IANA) or a temporary multicast address in a certain scenario. If the flag bit is 0, this address is a known multicast address. If the flag bit is 1, this address is a temporary multicast address. The remaining three flag bits are reserved for future use.

- Scope field

The scope field consists of four bits to indicate the multicast range. That is, a multicast group includes the local node, local link, local site, and any node in the IPv6 global address space.

- Group ID field

The group ID consists of 112 bits to identify a multicast group. A multicast ID can represent different groups based on the flag and scope fields.

IPv6 multicast addresses are prefixed with FF00::/8. One IPv6 multicast address usually identifies interfaces on a series of different nodes. After a packet is sent to a multicast address, the packet is then forwarded to the interfaces on each node identified by this multicast address. For a node (host or device), you must add the following multicast addresses:

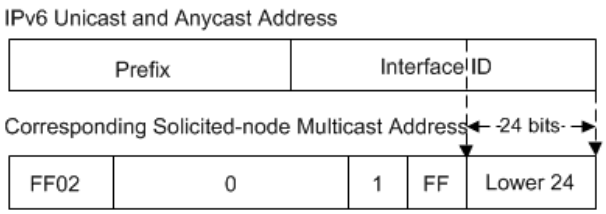
3. Multicast address for all nodes on the local link, that is, FF02::1
4. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

If the node is a device, it also has to be added to the multicast address of all devices on the local link, that is, FF02::2.

The solicited-node multicast address corresponds to the IPv6 unicast and anycast address. You must add a corresponding solicited-node multicast address for each configured unicast and anycast address of an IPv6 node. The solicited-node multicast address is prefixed with FF02:0:0:0:0:1:FF00:0000/104. The remaining 24 bits are composed of the least significant 24 bits of the unicast or anycast address. For example, if the unicast address is FE80::2AA:FF:FE21:1234, the solicited-node multicast address is FF02::1:FF21:1234.

The solicited-node multicast address is usually used in NS packets. Its address format is as follows:

Figure 3-7



Anycast Addresses

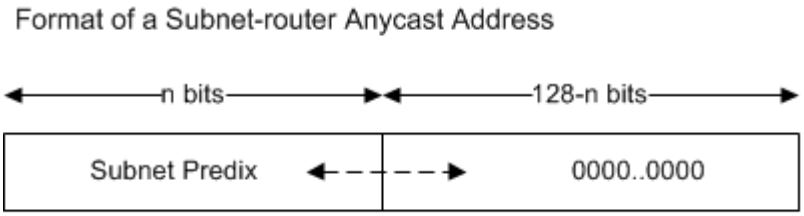
Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets while all nodes included in the multicast address receive data packets. Since anycast addresses are allocated to the normal IPv6 unicast address space, they have the same formats with unicast addresses. Every member in an anycast address must be configured explicitly for easier recognition.

Anycast addresses can be allocated only to devices and cannot be used as source addresses of packets.

RFC 2373 redefines an anycast address called subnet-router anycast address. Figure 3-8 shows the format of a subnet-router anycast address. Such an address consists of the subnet prefix and a series of 0s (interface ID).

The subnet prefix identifies a specified link (subnet). Packets destined to the subnet-router anycast address will be forwarded to a device on this subnet. A subnet-router anycast address is usually used by the application on a node to communicate with a device on a remote subnet.

Figure 3-8



Related Configuration

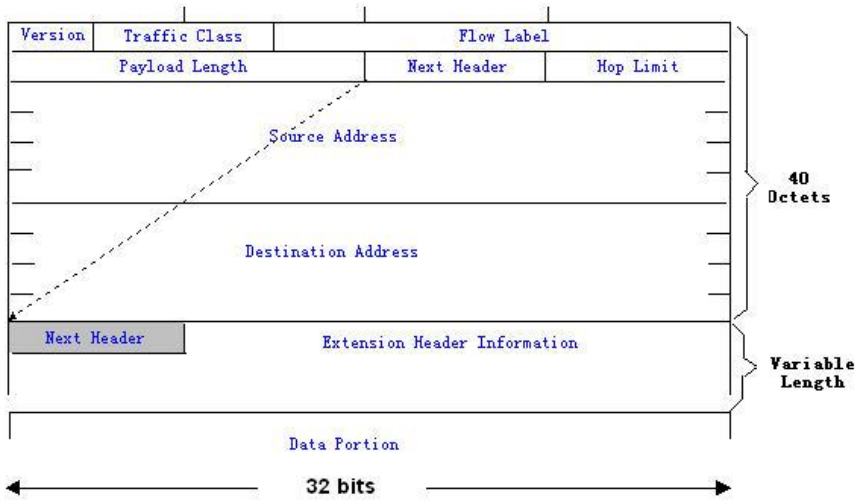
Configuring an IPv6 Address

- No IPv6 address is configured on interfaces by default.
- Run the **ipv6 address** command to configure the IPv6 unicast address and anycast address of an interface.
- After an interface goes up, it will automatically join the corresponding multicast group.

3.3.3 IPv6 Packet Header Format

Figure 3-9 shows the format of the IPv6 packet header.

Figure 3-9



The IPv4 packet header is in unit of four bytes. The IPv6 packet header consists of 40 bytes, in unit of eight bytes. The IPv6 packet header has the following fields:

- Version

This field consists of 4 bits. In an IPv6 address, this field must be 6.

- Traffic Class

This field consists of 8 bits. This field indicates the service provided by this packet, similar to the TOS field in an IPv4 address.

- Flow Label

This field consists of 20 bits to identify packets belonging to the same service flow. One node can act as the Tx source of multiple service flows. The flow label and source address uniquely identify one service flow.

- Payload Length

This field consists of 16 bits, including the packet payload length and the length of IPv6 extended options (if available). That is, it includes the IPv6 packet length except the IPv6 packet header.

- Next Header

This field indicates the protocol type in the header field following the IPv6 packet header. Similar to the Protocol field in the IPv4 address header, the Next Header field is used to indicate whether the upper layer uses TCP or UDP. It can also be used to indicate existence of the IPv6 extension header.

- Hop Limit

This field consists of 8 bits. Every time a device forwards a packet, the field value reduced by 1. If the field value reaches 0, this packet will be discarded. It is similar to the Lifetime field in the IPv4 packet header.

- Source Address

This field consists of 128 bits and indicates the sender address in an IPv6 packet.

- Destination Address

This field consists of 128 bits and indicates the receiver address in an IPv6 packet.

At present, IPv6 defines the following extension headers:

- Hop-By-Hop Options

This extension header must follow the IPv6 packet header. It consists of option data to be checked on each node along the path.

- Routing Options (Type 0 routing header)

This extension header indicates the nodes that a packet passes through from the source address to the destination address. It consists of the address list of the passerby nodes. The initial destination address in the IPv6 packet header is the first address among the addresses in the routing header, but not the final destination address of the packet. After the node corresponding to the destination address in the IPv6 packet header receives a packet, it processes the IPv6 packet header and routing header, and sends the packet to the second address, the third address, and so on in the routing header list till the packet reaches the final destination address.

- Fragment

The source node uses this extension header to fragment the packets of which the length exceeds the path MTU (PMTU).

- Destination Options

This extension header replaces the option fields of IPv4. At present, the Destination Options field can only be filled with integral multiples of 64 bits (eight bytes) if required. This extension header can be used to carry information to be checked by the destination node.

- Upper-layer header

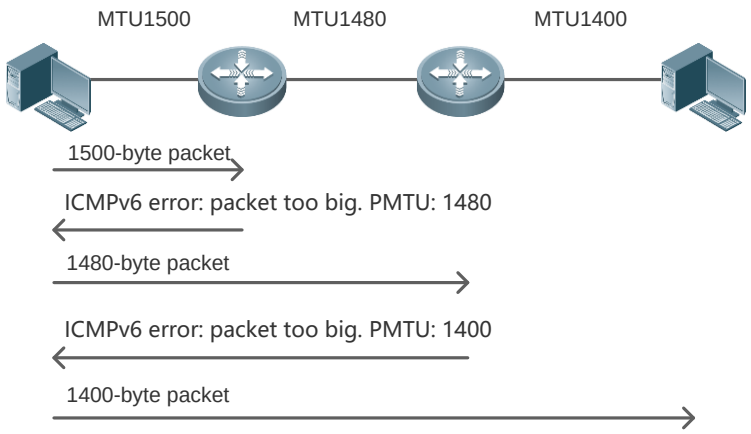
This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers AH and ESP will be described in the *Configuring IPSec*.

3.3.4 IPv6 PMTUD

Similar to IPv4 Path MTU Discovery (PMTUD), IPv6 PMTUD allows a host to dynamically discover and adjust the MTU size on the data Tx path. If the length of a data packet to be sent by a host is greater than the PMTU, the host performs packet fragmentation on its own. In this manner, the IPv6 device does not need to perform fragmentation, saving device resources and improving the IPv6 network efficiency.

Figure 3-10



As shown in Figure 3-10, if the length of a packet to be sent by the host is greater than the PMTU, the router discards this packet and sends an ICMPv6 Packet Too Big message containing its PMTU to the host. The host then fragments the packet based on the new PMTU. In this manner, the router does not need to perform fragmentation, saving router resources and improving the IPv6 network efficiency.

Related Configuration

Configuring the IPv6 MTU of an Interface

- The default IPv6 MTU is 1500 on an Ethernet interface.
- Run the **ipv6 mtu** command to modify the IPv6 MTU of an interface.

3.3.5 IPv6 Neighbor Discovery

NDP is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (like ARP), next-hop determination, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), ICMP Redirect (ICMP type: 137).

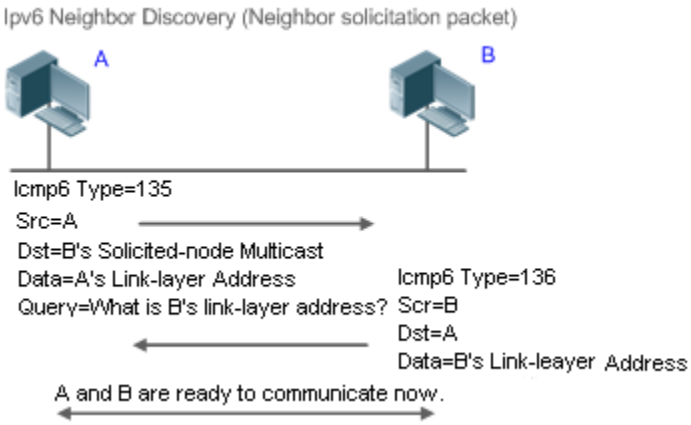
All the above ICMP packets carry one or multiple options. These options are optional in some cases but are significant in other cases. NDP mainly defines five options: Source Link-Layer Address Option, Type=1; Target Link-Layer Address Option, Type=2; Prefix Information Option, Type=3; Redirection Header Option, Type=4; MTU Option, Type=5.

Address Resolution

When a node attempts to communicate with another, the node has to obtain the link-layer address of the peer end by sending it an NS packet. In this packet, the destination address is the solicited-node multicast address corresponding to the IPv6 address of the destination node. This packet also contains the link-layer address of the source node. After receiving this NS packet, the peer end replies with an NA packet in which the destination address is the source address of the NS packet, that is, the link-layer address of the solicited node. After receiving this NA packet, the source node can communicate with the destination node.

Figure 3-11 shows the address resolution process.

Figure 3-11



NUD

If the reachable time of a neighbor has elapsed but an IPv6 unicast packet needs to be sent to it, the device performs NUD.

While performing NUD, the device can continue to forward IPv6 packets to the neighbor.

DAD

To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

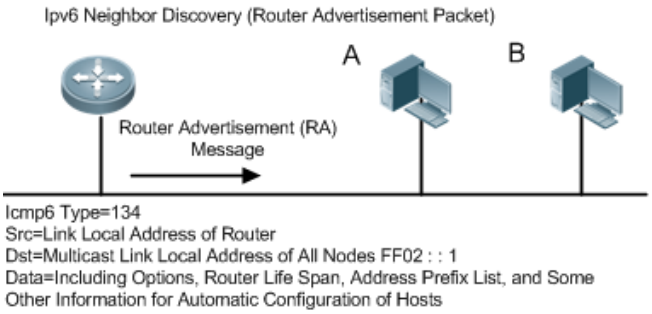
If a device detects an address conflict, this address is set to the duplicate status so that the device cannot receive IPv6 packets with this address being the destination address. Meanwhile, the device also starts a timer for this duplicate address to periodically perform DAD. If no address conflict is detected in re-detection, this address can be properly used.

Router, Prefix, and Parameter Discovery

A device periodically sends RA packets to all local nodes on the link.

Figure 3-12 shows the RA packet sending process.

Figure 3-12



An RA packet usually contains the following content:

- One or multiple IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
- Validity of the IPv6 address prefix

- Host auto-configuration method (stateful or stateless)
- Default device information (whether the device acts as the default device; if yes, the interval for acting as the default device is also included.)
- Other information provided for host configuration, such as hop limit, MTU, and NS retransmission interval

RA packets can also be used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately after started rather than wait for the RA packets sent by the device. If no unicast address is configured for a newly started host, the host includes the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (FF02::2) as the destination address in the RS packet. As an reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address (if the source address is the unspecified address, it uses the multicast address of all local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

- Ra-interval: Interval for sending the RA packet.
- Ra-lifetime: Lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
- Prefix: Prefix of an IPv6 address on the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
- Ns-interval: NS packet retransmission interval.
- Reachabletime: Period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
- Ra-hoplimit: Hops of the RA packet, used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: MTU of the RA packet.
- Managed-config-flag: Whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: Whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

Configure the above parameters when configuring IPv6 interface attributes.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time.

Maximum Number of Unresolved ND Entries

- You can configure the maximum number of unresolved ND entries to prevent malicious scanning network segments from generating a large number of unresolved ND entries and occupying excessive memory space.

Maximum Number of ND Options

- You can configure the maximum number of ND options to prevent forged ND packets from carrying unlimited ND options and occupying excessive CPU space on the device.

Maximum Number of Neighbor Learning Entries on an Interface

- You can configure the maximum number of neighbor learning entries on an interface to prevent neighbor learning attacks from occupying ND entries and memory space of the device and affecting forwarding efficiency of the device.

Related Configuration

Enabling IPv6 Redirection

- By default, ICMPv6 Redirect packets can be sent on IPv6 interfaces.
- Run the **no ipv6 redirects** command in interface configuration mode to prohibit an interface from sending Redirect packets.

Configuring IPv6 DAD

- By default, an interface sends one NS packet to perform IPv6 DAD.
- Run the **ipv6 nd dad attempts** *value* command in interface configuration mode to configure the number of NS packets consecutively sent by DAD. Value 0 indicates disabling DAD for IPv6 addresses on this interface.
- Run the **no ipv6 nd dad attempts** command to restore the default configuration.
- By default, the device performs DAD on duplicate IPv6 addresses every 60 seconds.
- Run the **ipv6 nd dad retry** value command in global configuration mode to configure the DAD interval. Value 0 indicates disabling DAD for the device.
- Run the **no ipv6 nd dad retry** command to restore the default configuration.

Configuring the Reachable Time of a Neighbor

- The default reachable time of an IPv6 neighbor is 30s.
- Run the **ipv6 nd reachable-time** *milliseconds* command in interface configuration mode to modify the reachable time of a neighbor.

Configuring the Stale Time of a Neighbor

- The default stale time of an IPv6 neighbor is 1 hour. After the time elapses, the device performs NUD.
- Run the **ipv6 nd stale-time** *seconds* command in interface configuration mode to modify the stale time of a neighbor.

Configuring Prefix Information

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- Run the **ipv6 nd prefix** command in interface configuration mode to add or delete prefixes and prefix parameters that can be advertised.

Enabling/disabling RA Suppression

- By default, an IPv6 interface does not send RA packets.
- Run the **no ipv6 nd suppress-ra** command in interface configuration mode to disable RA suppression.

Configuring the Maximum Number of Unresolved ND Entries

- The default value is 0, indicating no restriction. It is only restricted to the ND entry capacity supported by the device.
- Run the **ipv6 nd unresolved** *number* command in global configuration mode to restrict the number of unresolved neighbors. After the entries exceed this restriction, the device does not actively resolve subsequent packets.

Configuring the Maximum Number of ND Entries Learned on an Interface

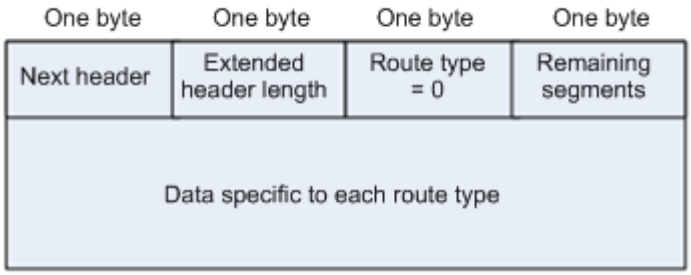
- Run the **ipv6 nd cache interface-limit** *value* command in interface configuration mode to restrict the number of neighbors learned on an interface. The default value is 0, indicating no restriction.

3.3.6 IPv6 Source Routing

Working Principle

Similar to the IPv4 loose source routing and loose record routing options, the IPv6 routing header is used to specify the intermediate nodes that the packet passes through along the path to the destination address. It uses the following format:

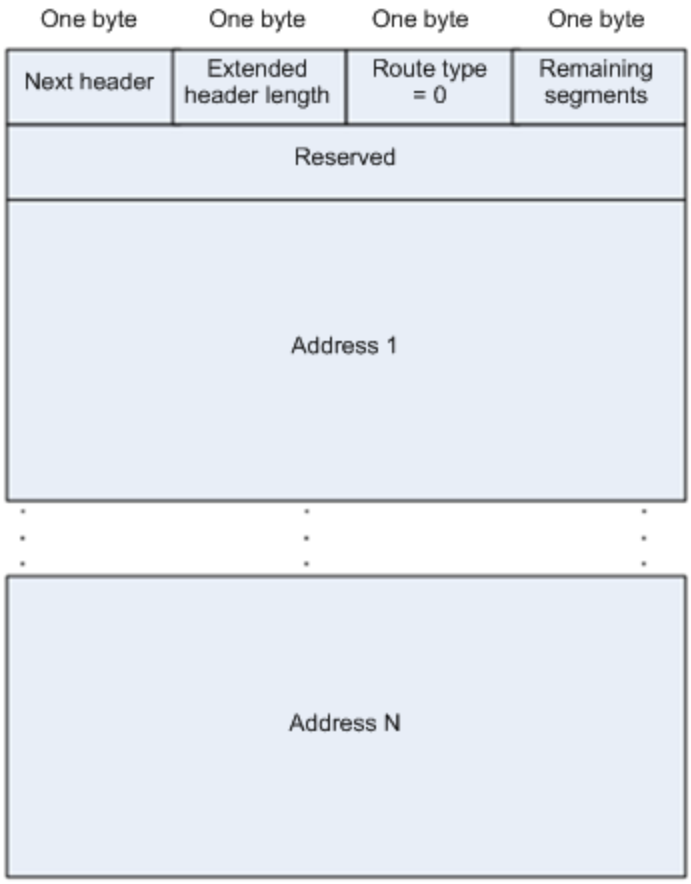
Figure 3-13



The Segments Left field is used to indicate how many intermediate nodes are specified in the routing header for the packet to pass through from the current node to the final destination address.

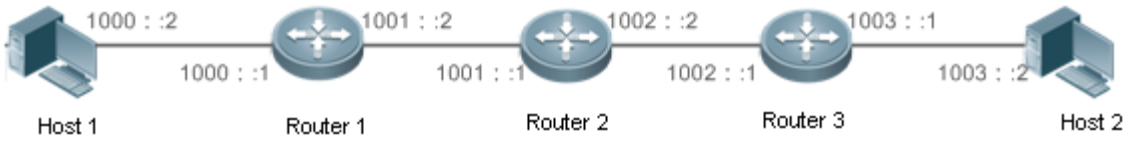
Currently, two routing types are defined: 0 and 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4). The format of the Type 0 routing header is as follows:

Figure 3-14



The following example describes the application of the Type 0 routing header, as shown in Figure 3-15.

Figure 3-15



Host 1 sends Host 2 a packet specifying the intermediate nodes Router 2 and Router 3. The following table lists the changes of fields related to the IPv6 header and routing header during the forwarding process.

Transmission Node	Fields in the IPv6 Header	Fields Related to the Type 0 Routing Header
Host 1	Source address=1000::2 Destination address=1001::1 (Address of Router 2)	Segments Left=2 Address 1=1002::1 (Address of Router 3) Address 2=1003::2 (Address of Host 2)
Router 1	No change	
Router 2	Source address=1000::2 Destination address=1002::1 (Address of Router 3)	Segments Left=1 Address 1=1001::1 (Address of Router 2) Address 2=1003::2 (Address of Host 2)

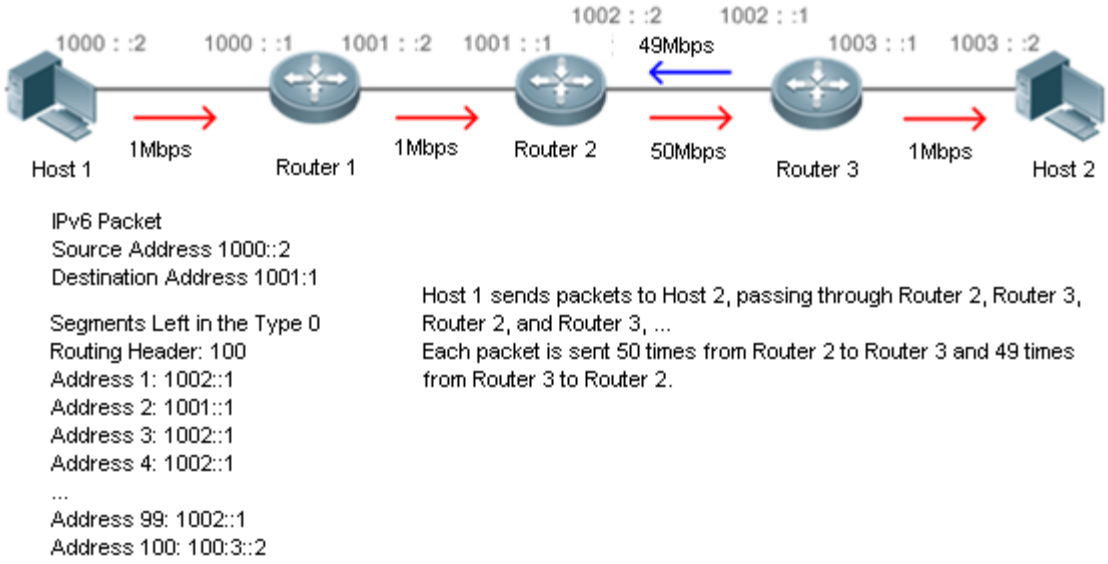
Router 3	Source address=1000::2 Destination address=1003::2 (Address of Host 2)	Segments Left=0 Address 1=1001::1 (Address of Router 2) Address 1=1002::2 (Address of Router 3)
Host 2	No change	

The forwarding process is as follows:

5. Host 1 sends a packet in which the destination address is Router 2's address 1001::1, the Type 0 routing header is filled with Router 3's address 1002::1 and Host 2's address 1003::2, and the value of the Segments Left field is 2.
6. Router 1 forwards this packet to Router 2.
7. Router 2 changes the destination address in the IPv6 header to Address 1 in the routing header. That is, the destination address becomes Router 3's address 1002::1, Address 1 in the routing header becomes Router 2's address 1001::1, and the value of the Segments Left field becomes 1. After modification, Router 2 forwards the packet to Router 3.
8. Router 3 changes the destination address in the IPv6 header to Address 2 in the routing header. That is, the destination address becomes Host 2's address 1003::2, Address 2 in the routing header becomes Router 3's address 1002::1, and the value of the Segments Left field becomes 0. After modification, Router 3 forwards the packet to Host 2.

The Type 0 routing header may be used to initiate DoS attacks. As shown in Figure 3-16, Host 1 sends packets to Host 2 at 1 Mbps and forges a routing header to cause multiple round-trips between Router 2 and Router 3 (50 times from Router 2 to Router 3 and 49 times from Router 3 to Router 2). At the time, the routing header generates the traffic amplification effect:" 50 Mbps from Router 2 to Router 3 and 49 Mbps from Router 3 to Router 2." Due to this security problem, RFC 5095 abolished the Type 0 routing header.

Figure 3-16



Related Configuration

Enabling IPv6 Source Routing

- The Type 0 routing header is not supported by default.
- Run the **ipv6 source-route** command in global configuration mode to enable IPv6 source routing.

3.3.7 Restricting the Sending Rate of ICMPv6 Error Messages

Working Principle

The destination node or intermediate router sends ICMPv6 error messages to report the errors incurred during IPv6 data packet forwarding and transmission. There are mainly four types of error messages: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problem.

When receiving an invalid IPv6 packet, a device discards the packet and sends back an ICMPv6 error message to the source IPv6 address. In the case of invalid IPv6 packet attacks, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to properly provide services. To solve this problem, you can restrict the sending rate of ICMPv6 error messages.

If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If the sending rate of ICMPv6 error messages is restricted due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages.

Although ICMPv6 Redirect packets are not ICMPv6 error messages, Ruijie recommends restricting their rates together with ICMPv6 error messages except Packet Too Big messages.

Related Configuration

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval too-big** command to configure the sending rate of ICMPv6 Packet Too Big messages.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval** command to configure the sending rate of other ICMPv6 error messages.

3.3.8 IPv6 Hop Limit

Working Principle

An IPv6 data packet passes through routers from the source address and destination address. If a hop limit is configured, it decreases by one every time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent this useless packet from being unlimitedly transmitted on the network and wasting network bandwidth. The hop limit is similar to the TTL of IPv4.

Related Configuration

Configuring the IPv6 Hop Limit

- The default IPv6 hop limit of a device is 64.
- Run the **ipv6 hop-limit** command to configure the IPv6 hop limit of a device.

3.3.9 Default Gateway on the Management Interface

Working Principle

The default gateway is configured on the management interface to generate a default route for this interface.

Related Configuration

Configuring the Default Gateway on the Management Interface

- Run the **ipv6 gateway** *ipv6-address* command in interface configuration mode to configure the default gateway on the management interface.
- No default gateway is configured on the management interface by default.

3.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address	(Mandatory) It is used to configure IPv6 addresses and enable IPv6.	
	ipv6 enable	Enables IPv6 on an interface.
	ipv6 address	Configures the IPv6 unicast address of an interface.
Configuring IPv6 NDP	(Optional) It is used to enable IPv6 redirection on an interface.	
	ipv6 redirects	Enables IPv6 redirection on an interface.
	(Optional) It is used to enable DAD.	
	ipv6 nd dad attempts	Configures the number of consecutive NS packets sent during DAD.
	(Optional) It is used to configure ND parameters.	
	ipv6 nd reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.
	ipv6 nd suppress-ra	Enables RA suppression on an interface.
	(Optional) It is used to configure the maximum number of unresolved ND entries.	
	ipv6 nd unresolved	Configures the maximum number of unresolved ND entries.

Configuration	Description and Command	
	(Optional) It is used to configure the maximum number of neighbors learned on an interface.	
	ipv6 nd cache interface-limit	Configures the maximum number of neighbors learned on an interface.
Enabling PMTUD	(Optional) It is used to restrict the MTU of IPv6 packets sent on an interface.	
	ipv6 mtu	Configures the IPv6 MTU.
Enabling IPv6 Source Routing	(Optional) It is used to enable IPv6 source routing.	
	ipv6 source-route	Configures the device to forward IPv6 packets carrying the routing header.
Configuring the Sending Rate of ICMPv6 Error Messages	Optional.	
	ipv6 icmp error-interval too-big	Configures the sending rate of ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the sending rates of other ICMPv6 error messages and ICMPv6 Redirect packets.
Configuring the IPv6 Hop Limit	(Optional) It is used to restrict the hop limit of IPv6 unicast packets sent on an interface.	
	ipv6 hop-limit	Configures the IPv6 hop limit.
Configuring the Default Gateway on the Management Interface	(Optional) It is used to configure the default gateway on the management interface.	
	ipv6 gateway *ipv6-address*	Configures the default gateway on the management interface.

3.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Steps

Enabling IPv6 on an Interface

- (Optional) If you do not want to enable IPv6 by configuring an IPv6 address, run the **ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

- Mandatory.

Verification

Run the **show ipv6 interface** command to check whether the configured address takes effect.

Related Commands

Enabling IPv6 on an Interface

Command	**ipv6 enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	IPv6 can be enabled on an interface by two methods: 1) running the **ipv6 enable** command in interface configuration mode; 2) configuring an IPv6 address on the interface. If an IPv6 address is configured on an interface, IPv6 is automatically enabled on this interface. In this case, IPv6 cannot be disabled even when you run the **no ipv6 enable** command.

Configuring the IPv6 Unicast Address of an Interface

Command	**ipv6 address** *ipv6-address* / *prefix-length* **ipv6 address** *ipv6-prefix* / *prefix-length* **eui-64** **ipv6 address** *prefix-name sub-bits* / *prefix-length* [**eui-64**]
Parameter Description	*ipv6-address*: Indicates the IPv6 address, which must comply with the address format defined in RFC 4291. Separated by a colon (:), each address field consists of 16 bits and is represented by hexadecimal digits. *ipv6-prefix*: Indicates the IPv6 address prefix, which must comply with the address format defined in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix, that is, the part representing the network in the IPv6 address. *prefix-name*: Indicates the name of the universal prefix. This specified universal prefix is used to create the interface address. *sub-bits*: Indicates the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* parameter. This value is combined with the universal prefix to create the interface address. This value must be in the form documented in RFC 4291. *eui-64*: Indicates the created IPv6 address, consisting of the configured address prefix and 64-bit interface ID.
Command Mode	Interface configuration mode
Usage Guide	If an IPv6 interface is created and is Up state, the system automatically generates a link-local address for this interface. The IPv6 address of an interface can also be created by the universal prefix mechanism. That is, IPv6 address = Universal prefix + Sub prefix + Host bits. The universal prefix can be configured by running the **ipv6 general-prefix** command or learned by the prefix discovery function of the DHCPv6 client (see the *Configuring DHCPv6*). Sub prefix + Host bits are specified by the *sub-bits* and *prefix-length* parameters in the **ipv6 address** command. If you run the **no ipv6 address** command without specifying an address, all manually configured addresses will be deleted.

	Run the **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** command to delete the configured address.

Configuration Example

Configuring an IPv6 Address on an Interface

Configuration Steps	Enable IPv6 on the GigabitEthernet 0/0 interface and add IPv6 address 2000::1 to the interface.
	Ruijie(config)#interface gigabitEthernet 0/0 Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
Verification	Run the **show ipv6 interface** command to verify that an address is successfully added to the GigabitEthernet 0/0 interface.
	Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 INET6: 2000::1 [TENTATIVE], subnet is 2000::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

3.4.2 Configuring IPv6 NDP

Configuration Effect

Configure NDP-related attributes, for example, enable IPv6 redirection and DAD.

Notes

RA suppression is enabled on interfaces by default. To configure a device to send RA packets, run the **no ipv6 nd suppress-ra** command in interface configuration mode.

Configuration Steps

Enabling IPv6 Redirection on an Interface

- (Optional) IPv6 redirection is enabled by default.
- To disable IPv6 redirection on an interface, run the **no ipv6 redirects** command.

Configuring the Number of Consecutive NS Packets Sent During DAD

- Optional.
- To prevent enabling DAD for IPv6 addresses on an interface or modify the number of consecutive NS packets sent during DAD, run the **ipv6 nd dad attempts** command.

Configuring the Reachable Time of a Neighbor

- Optional.
- To modify the reachable time of a neighbor, run the **ipv6 nd reachable-time** command.

Configuring the Address Prefix to Be Advertised in an RA Packet

- By default, the prefix in an RA packet on an interface is the prefix configured in the **ipv6 address** command on the interface.
- (Optional) Run the **ipv6 nd prefix** command to add or delete prefixes and prefix parameters that can be advertised. Or run the **peer default ipv6 pool** command to assign a prefix from the prefix pool for advertisement

Enabling/Disabling RA Suppression on an Interface

- Optional.
- If a device needs to send RA packets, run the **no ipv6 nd suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

- Optional.
- If a large number of unresolved ND entries are generated due to scanning attacks, run the **ipv6 nd unresolved** command to restrict the number of unresolved neighbors.

Configuring the Maximum Number of ND Options

- Optional.
- If a device needs to process more options, run the **ipv6 nd max-opt** command.

Configuring the Maximum Number of ND Entries Learned on an Interface

- Optional.
- If the number of IPv6 hosts is controllable, run the **ipv6 nd cache interface-limit** command to restrict the number of neighbors learned on an interface. This prevents ND learning attacks from occupying the memory space and affecting device performance.

Verification

Run the following commands to check whether the configuration is correct:

- **show ipv6 interface** *interface-type interface-num*: Check whether the configurations such as the redirection function, reachable time of a neighbor, and NS sending interval take effect.
- **show ipv6 interface** *interface-type interface-num* **ra-inifo**: Check whether the prefix and other information configured for RA packets are correct.
- **show run**

Related Commands

Enabling IPv6 Redirection on an Interface

Command	**ipv6 redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited transmission rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	**ipv6 nd dad attempts** *value*
Parameter Description	*value*: Indicates the number of NS packets.
Command Mode	Interface configuration mode
Usage Guide	You need to enable DAD before configuring an IPv6 address on an interface. Then the address is in tentative state. If no address conflict is detected by DAD, this address can be correctly used. If an address conflict is detected and the interface ID of this address uses EUI-64, duplicate link-layer addresses exist on this link. In this case, the system automatically disables this interface to prevent IPv6-related operations on this interface). At the time, you must configure a new address and restart the interface to re-enable DAD. When an interface changes from the down state to the up state, DAD is re-enabled for the addresses on this interface.

Configuring the Reachable Time of a Neighbor

Command	**ipv6 nd reachable-time** *milliseconds*

Parameter Description	*milliseconds*: Indicates the reachable time of a neighbor, ranging from 0 to 3,600,000. The unit is millisecond. The default value is 30s.
Command Mode	Interface configuration mode
Usage Guide	A device detects unreachable neighbors based on the configured reachable time. The shorter the configured reachable time, the faster the device detects unreachable neighbors but the more it consumes network bandwidth and device resources. Therefore, it is not recommended to set this time too small. The configured value is advertised in an RA packet and is also used on the device. If the value is 0, the reachable time is not specified on the device and it is recommended to use the default value.

Configuring the Address Prefix to Be Advertised in an RA Packet

Command	**ipv6 nd prefix {***ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]
Parameter Description	*ipv6-prefix*: Indicates the network ID of IPv6, which must comply with the address representation format in RFC 4291. *prefix-length*: Indicates the length of the IPv6 address prefix. A slash (/) must be added before the prefix. *valid-lifetime*: Indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 30 days. *preferred-lifetime*: Indicates the preferred period when a host receiving the prefix of an RA packet regards the prefix valid. The value ranges from 0 to 4,294,967,295. The default value is 7 days. **at** *valid-date preferred-date*: Indicates the valid date and preferred deadline configured for the RA prefix. It uses the format of *dd+mm+yyyy+hh+mm*. **infinite**: Indicates that the prefix is permanently valid. **default**: Indicates that the default parameter configuration is used. **no-advertise**: Indicates that the prefix is not advertised by a router. **off-link**: If the prefix of the destination address in the IPv6 packet sent by a host matches the configured prefix, the device regards the destination address on the same link and directly reachable. This parameter indicates that this prefix does not require on-link determination. **no-autoconfig**: Indicates that the prefix in the RA packet received by a host cannot be used for address auto-configuration.
Command Mode	Interface configuration mode
Usage Guide	This command can be used to configure parameters related to each prefix, including whether to advertise this prefix. By default, an RA packet uses the prefix configured by running the **ipv6 address** command. Run the **ipv6 nd prefix** command to add other prefixes. Run the **ipv6 nd prefix default** command to configure the default parameters for an interface. That is, if no parameter is specified when a prefix is added, use the parameters configured in the **ipv6 nd prefix default** command as the parameters of the new prefix. The default parameter configurations are abandoned once a parameter is specified for the prefix. That is, when you use the **ipv6 nd prefix default** command to modify the default parameter configurations, only the prefix configured for the default parameters changes and

	configurations of the prefix remain the same. **at** *valid-date preferred-date*: You can specify the valid date of the prefix in two methods: 1) specifying a fixed time for each prefix in an RA packet; 2) specifying the deadline. In the second method, the valid date of the prefix in each RA packet decreases till it becomes 0.

Enabling/Disabling RA Suppression on an Interface

Command	**ipv6 nd suppress-ra**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To enable RA suppression on an interface, run the **ipv6 suppress-ra** command.

Configuring the Maximum Number of Unresolved ND Entries

Command	**ipv6 nd unresolved** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ND entries.
Command Mode	Global configuration mode
Usage Guide	To prevent malicious scanning attacks from creating a large number of unresolved ND entries and occupying entry resources, you can restrict the number of unresolved ND entries.

Configuring the Maximum Number of ND Entries Learned on an Interface

Command	**ipv6 nd cache interface-limit** *value*
Parameter Description	*value*: Indicates the maximum number of neighbors learned by an interface.
Command Mode	Interface configuration mode
Usage Guide	Restricting the number of ND entries learned on an interface can prevent malicious neighbor attacks. If this number is not restricted, a large number of ND entries will be generated on the device, occupying excessive memory space. The configured value must be equal to or greater than the number of the ND entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ND entry capacity supported by the device.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	Enable IPv6 redirection on interface GigabitEthernet 0/0.
	`Ruijie(config-if-GigabitEthernet 0/0)#ipv6 redirects`

Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Ruijie#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes ICMP error messages limited to one every 100 milliseconds ICMP redirects are enabled ND DAD is enabled, number of DAD attempts: 1 ND reachable time is 30000 milliseconds ND advertised reachable time is 0 milliseconds ND retransmit interval is 1000 milliseconds ND advertised retransmit interval is 0 milliseconds ND router advertisements are sent every 200 seconds<160--240> ND router advertisements live for 1800 seconds

Configuring IPv6 DAD

Configuration Steps	Configure the interface to send three consecutive NS packets during DAD.
	Ruijie(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	Ruijie#show ipv6 interface gigabitEthernet 0/0 interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0 address(es): Mac Address: 00:00:00:00:00:00 INET6: FE80::200:FF:FE00:1 [TENTATIVE], subnet is FE80::/64 Joined group address(es): MTU is 1500 bytes

```
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
Ruijie(config-if-GigabitEthernet 0/0)#
```

Configuring Prefix Information in an RA Packet

Configuration Steps	Add a prefix 1234::/64 to interface GigabitEthernet 0/0.
	`Ruijie(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	`Ruijie#show ipv6 interface gigabitEthernet 0/0 ra-info` `GigabitEthernet 0/0: DOWN (RA is suppressed)` `  RA timer is stopped` `  waits: 0, initcount: 0` `  statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0` `  Link-layer address: 00:00:00:00:00:00` `  Physical MTU: 1500` `  ND router advertisements live for 1800 seconds` `  ND router advertisements are sent every 200 seconds<160--240>` `  Flags: !M!O, Adv MTU: 1500` `  ND advertised reachable time is 0 milliseconds` `  ND advertised retransmit time is 0 milliseconds` `  ND advertised CurHopLimit is 64` `  Prefixes: <total: 1>` `    1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)`

Configuring RA Packets to Obtain Prefixes from the Prefix Pool

Configuration Steps	Configure RA packets to obtain prefixes from the prefix pool "ra-pool".
	`Ruijie(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0` `Building configuration...` `Current configuration : 125 bytes` `interface GigabitEthernet 0/0` ` ipv6 enable` ` no ipv6 nd suppress-ra` `peel default ipv6 pool ra-pool` `!`

Disabling RA Suppression

Configuration Steps	Disable RA suppression on an interface.
	`Ruijie(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0` `Building configuration...` `Current configuration : 125 bytes` `interface GigabitEthernet 0/0` ` ipv6 enable` ` no ipv6 nd suppress-ra` `!`

Configuring the Maximum Number of Unresolved ND Entries

Configuration Steps	Set the maximum number of unresolved ND entries to 200.
	`Ruijie(config)# ipv6 nd unresolved 200`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Ruijie#show run` `ipv6 nd unresolved 200` `!`

Configuring the Maximum Number of ND Entries Learned on an Interface

Configuration Steps	Set the maximum number of ND entries learned on an interface to 100.
	`Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Ruijie#show run` `!` `interface GigabitEthernet 0/1` `ipv6 nd cache interface-limit 100` `!`

3.4.3 Enabling PMTUD

Configuration Effect

When sending an IPv6 packet, a host fragments the packet based on the PMTU.

Notes

The IPv6 MTU of an interface must be less than or equal to the interface MTU.

Configuration Steps

Configuring the IPv6 MTU of an Interface

- Optional.

Verification

- Run the **show run** command to check whether the configuration is correct.

- Run the **show ipv6 interface** command to check whether the IPv6 MTU of an interface is correct.
- Capture the locally sent IPv6 packets of which the length exceeds the PMTU. The packet capture result shows that the IPv6 packet is fragmented based on the PMTU.

Related Commands

Configuring the IPv6 MTU of an Interface

Command	**ipv6 mtu** *bytes*
Parameter Description	*bytes*: Indicates the MTU of an IPv6 packet, ranging from 1280 to 1500. The unit is byte.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring the IPv6 MTU of an Interface

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.
	`Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	`Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface` `interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0` `  address(es):` `    Mac Address: 00:d0:f8:22:33:47` `    INET6: FE80::2D0:F8FF:FE22:3347 [ TENTATIVE ], subnet is FE80::/64` `    INET6: 1020::1 [ TENTATIVE ], subnet is 1020::/64` `    INET6: 1023::1 [ TENTATIVE ], subnet is 1023::/64` `  Joined group address(es):` `  MTU is 1300 bytes` `  ICMP error messages limited to one every 100 milliseconds` `  ICMP redirects are enabled` `  ND DAD is enabled, number of DAD attempts: 1` `  ND reachable time is 30000 milliseconds` `  ND advertised reachable time is 0 milliseconds`

Configuration Steps	Change the IPv6 MTU of interface GigabitEthernet 0/0 to 1,300.
	`Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300`
Verification	Run the **show ipv6 interface** command to check whether the configuration takes effect.
	`ND retransmit interval is 1000 milliseconds` `ND advertised retransmit interval is 0 milliseconds` `ND router advertisements are sent every 200 seconds<160--240>` `ND router advertisements live for 1800 seconds`

3.4.4 Enabling IPv6 Source Routing

Configuration Effect

RFC 5095 abolished the Type 0 routing header. Ruijie devices do not support the Type 0 routing header by default. The administrator can run the **ipv6 source-route** command to in global configuration mode to enable IPv6 source routing.

Configuration Steps

↘ Enabling IPv6 Source Routing

- Optional.
- To enable IPv6 source routing, run the **ipv6 source-route** command.

Verification

The device can properly forward packets carrying the Type 0 routing header.

Related Commands

↘ Enabling IPv6 Source Routing

Command	**ipv6 source-route**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Since the Type 0 header may cause the device prone to DoS attacks, the device does not forward IPv6 packets carrying the routing header by default, but still processes IPv6 packets with itself being the final destination address and the Type 0 routing header.

Configuration Example

↘ Enabling IPv6 Source Routing

Configuration Steps	Enable IPv6 source routing.
	`Ruijie(config)#ipv6 source-route`
Verification	Run the **show run** command to check whether the configuration takes effect.
	`Ruijie#show run | inc ipv6 source-route` `ipv6 source-route`

3.4.5 Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Effect

Configure the sending rate of ICMPv6 error messages.

Configuration Steps

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

- Optional.
- If a device receives many IPv6 packets with the packet length exceeding the IPv6 MTU of the outbound interface and thereby sends many ICMPv6 Packet Too Big messages to consume much CPU resources, run the **ipv6 icmp error-interval too-big** command to restrict the sending rate of this error message.

Configuring the Sending Rate of Other ICMPv6 Error Messages

- Optional.
- If a device receives many illegal IPv6 packets and thereby generates many ICMPv6 error messages, run the **ipv6 icmp error-interval** command to restrict the sending rate of ICMPv6 error messages. (This command does not affect the sending rate of ICMPv6 Packet Too Big messages.)

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Sending Rate of ICMPv6 Packet Too Big Messages

Command	**ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command	Global configuration mode

Mode	
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. If the length of an IPv6 packet to be forwarded exceeds the IPv6 MTU of the outbound interface, the router discards this IPv6 packet and sends back an ICMPv6 Packet Too Big message to the source IPv6 address. This error message is mainly used as part of the IPv6 PMTUD process. If other ICMPv6 error messages are excessive, ICMPv6 Packet Too Big messages cannot be sent, causing failure of IPv6 PMTUD. Therefore, it is recommended to restrict the sending rate of ICMPv6 Packet Too Big messages independently of other ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuring the Sending Rate of Other ICMPv6 Error Messages

Command	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, ranging from 0 to 2,147,483,647. The unit is millisecond. The default value is 100. If the value is 0, the sending rate of ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket, ranging from 1 to 200. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	To prevent DoS attacks, use the token bucket algorithm to restrict the sending rate of ICMPv6 error messages. Since the precision of the timer is 10 milliseconds, it is recommended to set the refresh period of a token bucket to an integer multiple of 10 milliseconds. If the refresh period of the token bucket is between 0 and 10, the actual refresh period is 10 milliseconds. For example, if the sending rate is set to 1 every 5 milliseconds, two error messages are sent every 10 milliseconds in actual situations. If the refresh period of the token bucket is not an integer multiple of 10 milliseconds, it is automatically converted to an integer multiple of 10 milliseconds. For example, if the sending rate is set to 3 every 15 milliseconds, two tokens are refreshed every 10 milliseconds in actual situations.

Configuration Example

Configuring the Sending Rate of ICMPv6 Error Messages

Configuration Steps	Set the sending rate of the ICMPv6 Packet Too Big message to 100 pps and that of other ICMPv6 error messages to 10 pps.

	Ruijie(config)#ipv6 icmp error-interval too-big 1000 100 Ruijie(config)#ipv6 icmp error-interval 1000 10
Verification	Run the **show running-config** command to check whether the configuration takes effect.
	Ruijie#show running-config | include ipv6 icmp error-interval ipv6 icmp error-interval 1000 10 ipv6 icmp error-interval too-big 1000 100

3.4.6 Configuring the IPv6 Hop Limit

Configuration Effect

Configure the number of hops of a unicast packet to prevent the packet from being unlimitedly transmitted.

Configuration Steps

Configuring the IPv6 Hop Limit

- Optional.
- To modify the number of hops of a unicast packet, run the **ipv6 hop-limit value** command.

Verification

- Run the **show running-config** command to check whether the configuration is correct.
- Capture the IPv6 unicast packets sent by a host. The packet capture result shows that the hop-limit field value in the IPv6 header is the same as the configured hop limit.

Related Commands

Configuring the IPv6 Hop Limit

Command	**ipv6 hop-limit value**
Parameter Description	*value*: Indicates the number of hops of a unicast packet sent by the device. The value ranges from 1 to 255.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the IPv6 Hop Limit

Configuration Steps	Change the IPv6 hop limit of a device to 250.
	Ruijie(config)#ipv6 hop-limit 250

Verification	Run the **show running-config** command to check whether the configuration takes effect.
	`Ruijie#show running-config` `ipv6 hop-limit 254`

3.4.7 Configuring the Default Gateway on the Management Interface

Configuration Effect

Configure the default gateway on the management interface. A default route is generated, with the outbound interface being the management interface and the next hop being the configured gateway.

Notes

The configuration is supported only on the management interface.

Configuration Steps

Configuring the Default Gateway on the Management Interface

- Optional.
- To configure a default route and the next hop for the management interface, run the **ipv6 gateway** command.

Verification

- Run the **show running-config** command to check whether the configuration is correct.

Related Commands

Configuring the Default Gateway on the Management Interface

Command	**ipv6 gateway** *ipv6-address*
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	This command is supported only on the management interface.

Configuration Example

Configuring the Default Gateway on the Management Interface

Configuration Steps	Sett the default gateway of the management interface to 2000::1.
	`Ruijie(config)# interface mgmt 0` `Ruijie(config-mgmt)# ipv6 gateway 2000::1`
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.

Configuration Steps	Sett the default gateway of the management interface to 2000::1.
	`Ruijie(config)# interface mgmt 0` `Ruijie(config-mgmt)# ipv6 gateway 2000::1`
Verification	Run the **show running-config interface vlan 2** command to check whether the configuration takes effect.
	`Ruijie#show running-config interface mgmt 0` `Ipv6 gateway 2000::1`

3.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the dynamically learned neighbors.	**clrear ipv6 neighbors** [*interface-id*]

Displaying

Description	Command
Displays IPv6 information of an interface.	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
Displays neighbor information.	**show ipv6 neighbors** [**verbose**] [*interface-id*] [*ipv6-address*] [static]

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs ND entry learning.	**debug ipv6 nd**

4 Configuring DHCP

4.1 Overview

The Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on the User Datagram Protocol (UDP) for dynamically assigning reusable network resources, for example, IP addresses.

The DHCP works in Client/Server mode. A DHCP client sends a request message to a DHCP server to obtain an IP address and other configurations. When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC3046: DHCP Relay Agent Information Option

4.2 Applications

Application	Description
Providing DHCP Service in a LAN	Assigns IP addresses to clients in a LAN.
Enabling DHCP Client	Enable DHCP Client.
Applying AM Rule on DHCP Server	Apply DHCP Server in Super VLAN environment.
Deploying DHCP Relay in WLAN	In a WLAN, users from different network segments requests IP addresses.
Applying AM Rule on DHCP Relay	In a Super VLAN, users from different network segments requests IP addresses.
Assigning DNS Addresses Obtained from External DHCP Server	In a WLAN, assign preferentially DNS addresses obtained from external DHCP server in WLAN.

4.2.1 Providing DHCP Service in a LAN

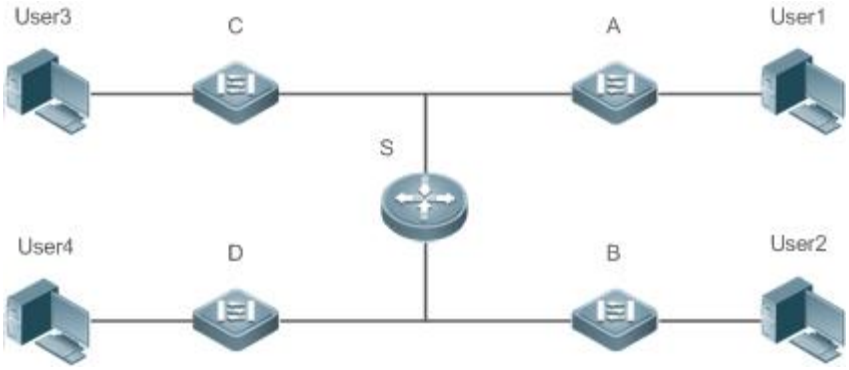
Scenario

Assign IP addresses to four users in a LAN.

For example, assign IP addresses to User 1, User 2, User 3 and User 4, as shown in the following figure.

- The four users are connected to Server S through A, B, C and D.

Figure 4-1



Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches achieving layer-2 transparent transmission. User 1, User 2, User 3 and User 4 are LAN users.

Deployment

- Enable DHCP Server on S.
- Deploy layer-2 VLAN transparent transmission on A, B, C and D.
- User 1, User 2, User 3 and User 4 initiate DHCP client requests.

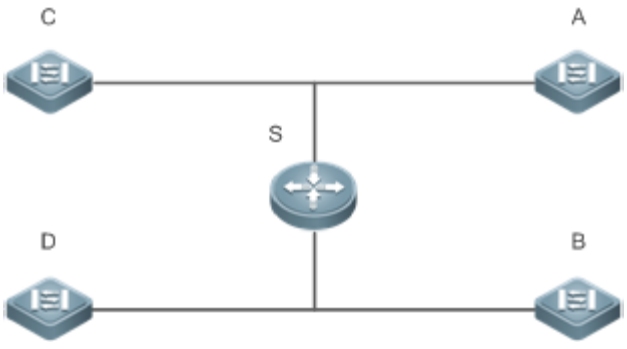
4.2.2 Enabling DHCP Client

Scenario

Access switches A, B, C and D in a LAN request server S to assign IP addresses.

For example, enable DHCP Client on the interfaces of A, B, C and D to request IP addresses, as shown in the following figure.

Figure 4-2



Remarks	S is an egress gateway working as a DHCP server. A, B, C and D are access switches with DHCP Client enabled on the interfaces.

Deployment

- Enable DHCP Server on S.
- Enable DHCP Client on the interfaces of A, B, C and D.

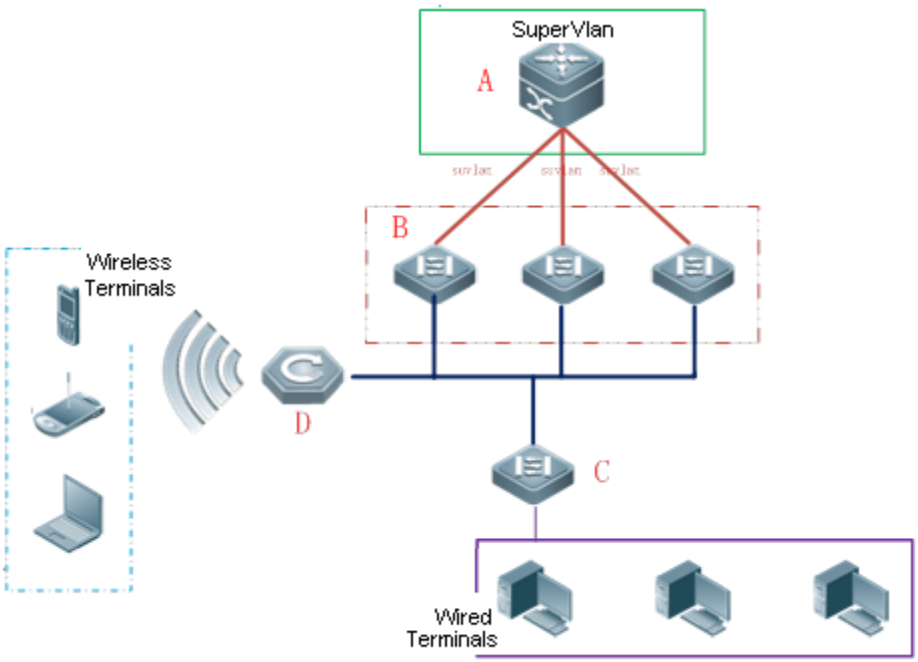
4.2.3 Applying AM Rule on DHCP Server

Scenario

As shown in Figure 4-3, create a Super VLAN, configure an AM rule and enable DHCP Server on the core switch A. B is an aggregation switch, C an access switch, and D a wireless access device. The requirements are listed as follows:

- Assign IP addresses dynamically based on the VLAN and port;
- Assign IP addresses statically based on the VLAN;
- Assign IP addresses dynamically based on the default AM rule.

Figure 4-3 Applying AM Rule on a DHCP Server



Remarks	A is a core device. B is an aggregation device. C is a wired access device. D is a wireless access device.

Deployment

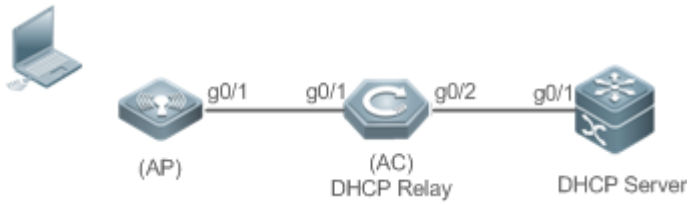
- Configure an AM rule, enable DHCP Server and create a Super VLAN on A.
- Create VLANs on B and C to transparently transmit DHCP packets from wired users to A to request IP addresses.
- Enable the wireless function on D to transparently transmit DHCP packets from wireless users to A to request IP addresses.

4.2.4 Deploying DHCP Relay in WLAN

Scenario

Wireless users in different network segments obtain IP addresses to access the Internet.

Figure 4-4 DHCP Relay



Remarks	AP is a wireless access point. AC is a wireless management device and DHCP Relay agent. DHCP Server is a core device responsible for assigning IP addresses to wireless users.

Deployment

- Connect AP to AC.
- Enable DHCP Relay on AC.
- Enable DHCP Server on the core device.

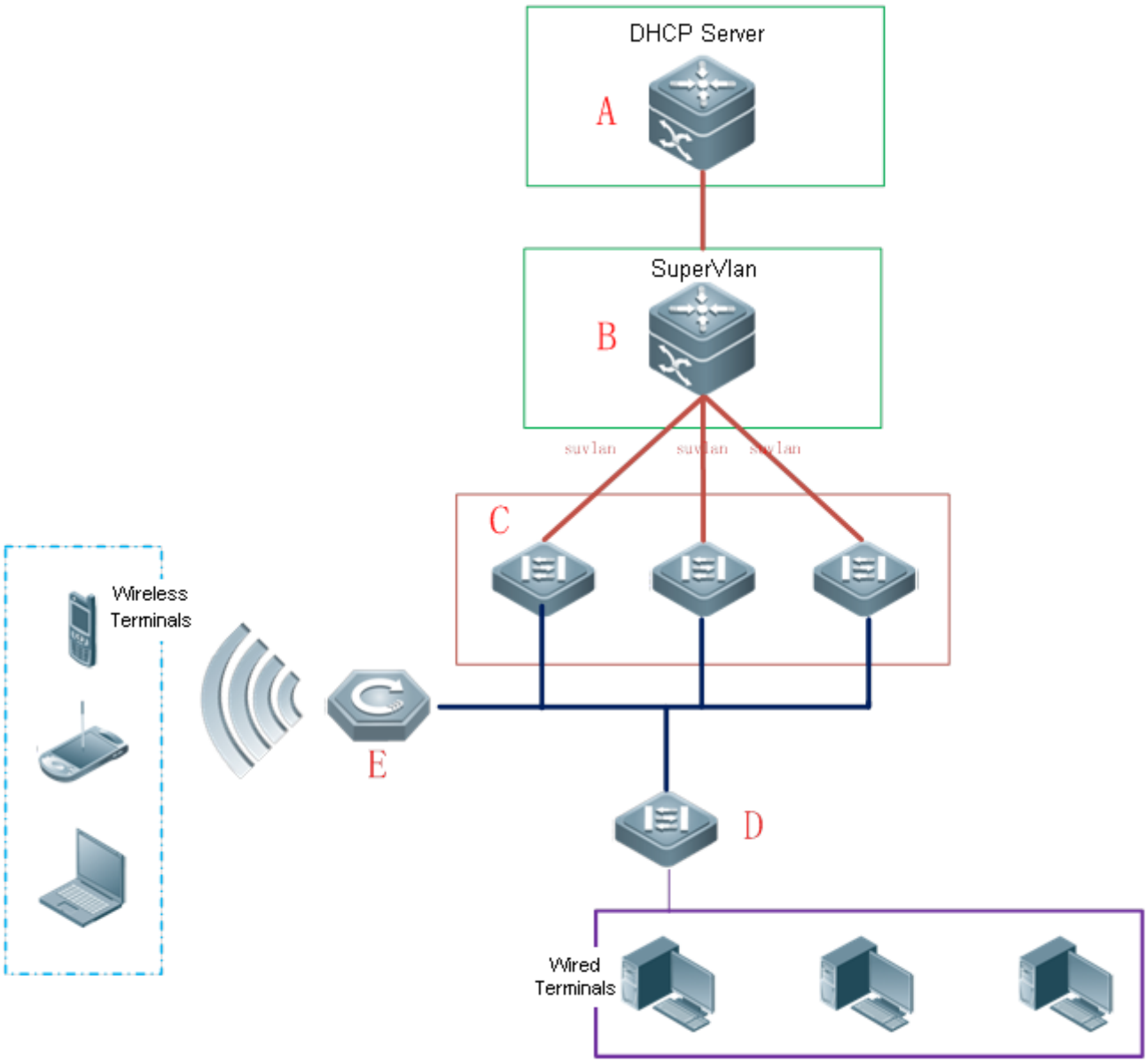
4.2.5 Applying AM Rule on DHCP Relay

Scenario

As shown in Figure 4-5, A is a DHCP server, B a core switch configured with Super VLAN, an AM rule and DHCP Relay, C an aggregation switch, D an access switch, and E a wireless access device. The requirements are listed as follows:

- Based on the VLAN-port AM rule, the DHCP relay agent chooses a subnet address as Giaddress of relay packets and forwards them to the DHCP server to request an IP address for the client.
- Based on default AM rule, the DHCP relay agent chooses a subnet address as Giaddress of relaying packets and forwards them to the DHCP server to request an IP address for the client.

Figure 4-5 Applying AM Rule on DHCP Relay



Remarks	A is a core device. B is a core device. C is an aggregation device. D is a wired access device. E is a wireless access device.

Deployment

- Enable DHCP Server on A.
- Configure an AM rule, enable DHCP Relay and create a Super VLAN on B.
- Create VLANs on C and D to transparently transmit DHCP packets from wired users to B to request IP addresses.

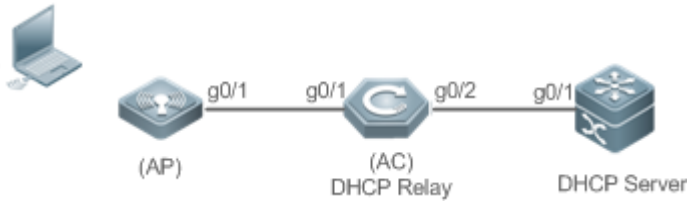
- Enable the wireless function on E to transparently transmit DHCP packets from wireless users to B to request IP addresses.

4.2.6 Assigning Preferentially DNS Addresses Obtained from External DHCP Server in WLAN

Scenario

When the WAN port of a wireless fat AP operates in PPPoE or DHCP Client mode, a DNS address can be automatically obtained from an external DHCP server and be configured on the DHCP server of the local device, so that the user does not need to perform DNS configuration. When the fat AP serves as the DHCP server, it preferentially assigns STAs with DNS addresses obtained from an external DHCP server.

Figure 4-6 DHCP Server Network Topology



Remarks	When an AP operates in fat AP mode, and the WAN port of the fat AP operates in PPPoE or DHCP Client mode, the AP can obtain IP addresses and DNS addresses from an external DHCP server, and serves as the DHCP server to assign addresses to STAs.

Deployment

- Configure the AP as a fat AP and enable the PPPoE or DHCP Client function on the WAN port of the fat AP.
- Enable the DHCP server function on the fat AP to assign addresses to STAs.
- Preferentially assign DNS addresses obtained by the PPPoE or DHCP Client module from an external DHCP server to STAs.

4.3 Features

Basic Concepts

↘ DHCP Server

Based on the RFC 2131, Ruijie DHCP server assigns IP addresses to clients and manages these IP addresses.

↘ DHCP Client

DHCP Client enables a device to automatically obtain an IP address and configurations from a DHCP server.

↘ DHCP Relay

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay to forward DHCP request and reply packets.

Lease

Lease is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address is active when leased to a client. Before a lease expires, a client needs to renew the lease through a server. When a lease expires or is deleted from a server, the lease becomes inactive.

Excluded Address

An excluded address is a specified IP address not assigned to a client by a DHCP server.

Address Pool

An address pool is a collection of IP addresses that a DHCP server may assign to clients.

Option Type

An option type is a parameter specified by a DHCP server when it provides lease service to a DHCP client. For example, a public option include the IP addresses of a default gateway (router), WINS server and a DNS server. DHCP server allows configuration of other options. Though most options are defined in the RFC 2132, you can add user-defined options.

Overview

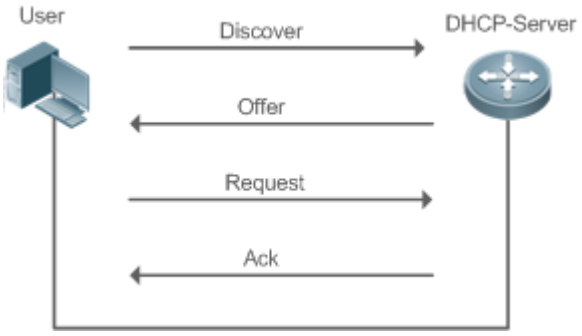
Feature	Description
DHCP Server	Enable DHCP Server on a device, and it may assign IP addresses dynamically and pushes configurations to DHCP clients.
DHCP Relay Agent	Enable DHCP Relay on a device, and it may forward DHCP request and reply packets across different network segments.
DHCP Client	Enable DHCP Client on a device, and it may obtain IP addresses and configurations automatically from a DHCP server.
AM Rule	Enable an AM rule on a device, and it may assign IP addresses according to the rule.

4.3.1 DHCP Server

Working Principle

DHCP Working Principle

Figure 4-7



A host requests an IP address through DHCP as follows:

9. A host broadcasts a DHCP discover packet to find DHCP servers in a network.
10. DHCP servers unicast/broadcast (based on the property of the host packet) DHCP offer packets to the host, containing an IP address, a MAC address, a domain name and a lease.
11. The host broadcasts a DHCP request packet to formally request an IP address.
12. A DHCP server sends a DHCP ACK unitcast packet to the host to acknowledge the request.

A DHCP client may receive DHCPOFFER packets from multiple DHCP servers, but usually it accepts only the first DHCPOFFER packet. Besides, the address specified in a DHCPOFFER packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a formal request.

To formally request an IP address, a client broadcasts a DHCPREQUEST packet so that all DHCP servers sending DHCPOFFER packets may receive the packet and release OFFER IP addresses.

If a DHCPOFFER packet contains invalid configuration parameters, a client will send a DHCPDECLINE packet to the server to decline the configuration.

During the negotiation, if a client does not respond to the DHCPOFFER packets in time, servers will send DHCPNAK packets to the client and the client will reinitiate the process.

During network construction, Ruijie DHCP servers have the following features:

- Low cost. Usually the static IP address configuration costs more than DHCP configuration.
- Simplified configuration. Dynamic IP address assignment dramatically simplifies device configuration
- Centralized management. You can modify the configuration for multiple subnets by simply modifying the DHCP server configuration.

Address Pool

After a server receives a client's request packet, it chooses a valid address pool, determines an available IP address from the pool through PING, and pushes the pool and address configuration to the client. The lease information is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters as follows:

- An IP address range, which is the range of IP addresses that are available.
- A gateway address. A maximum of 8 gateway addresses are supported.

- A DNS address. A maximum of 8 DNS addresses are supported.
- A lease period notifying clients of when to age an address and request a lease renewal.

VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, Ruijie devices enabled with DHCP provide a command to monitor the VRRP status of the interface. To an interface configured with VRRP address and VRRP monitoring, a DHCP server only processes the DHCP clients' request packets from the interface in Master state, and other packets are discarded. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP packets are processed. VRRP monitoring is configured on only layer-3 interfaces. It is disabled by default, namely, only the Master device processes the DHCP service.

IP Address Assignment Based on VLANs, Ports and IP Range

After an IP address pool is deployed, the specified IP address range is assigned based on VLANs and ports. There are three scenarios. 1. Global configuration. 2. Configuration based on VLANs, ports and IP range. 3. Both 1 and 2. In scenario 1, the addresses are assigned globally. In scenario 2, the addresses in the specified IP range are assigned only to the clients of the specified VLANs and ports. In scenario 3, the clients of the specified VLANs and ports are assigned the addresses in the specified IP range, and the other clients are configured with default global addresses.

Adding Trusted ARP

A trusted ARP prevents gateway ARP spoofing. Ruijie devices enabled with DHCP provide a command for pushing a trusted ARP while assigning an address. After this function is enabled, DHCP server pushes it while assigning an IP address to the client to prevent ARP spoofing.

ARP-Based Offline Detection

Ruijie devices enabled with DHCP provide a command to enable ARP-based offline detection. After this function is enabled, a DHCP server will receive an ARP aging notification when a client gets offline, and start retrieving the client's address. If the client does not get online within a period of time (5 minutes by default), the DHCP server will retrieve the address and assign it to another client. If the client gets online again, the address is still valid.

Adding Pseudo Server Detection

If a DHCP server is deployed illegally, a client interacts with this server while requesting an IP address and a wrong address will be assigned to the client. This server is a pseudo server. Ruijie devices enabled with DHCP provides a command to enable pseudo server detection. After it is enabled, DHCP packets are checked for Option 54 (Server Identifier Option). If the content of Option 54 is different from the actual DHCP server identifier, the IP address of the pseudo server and port receiving the packets will be recorded. The pseudo server detection is only an after-event security function and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

Related Configuration

Enabling DHCP Server Globally

- By default, DHCP Server is disabled.

- Run the **service dhcp** command to enable the DHCP Server.
- Run the **service dhcp** command globally to enable DHCP service.

↘ Configuring Address Pool

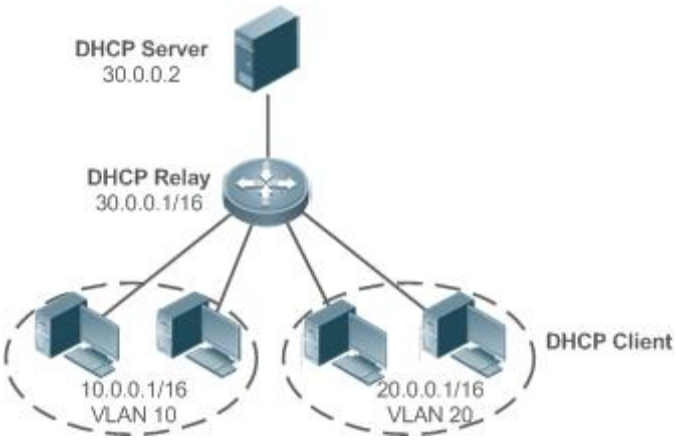
- By default, no address pool is configured.
- Run the **ip dhcp pool** command to configure an IP address range, a gateway and a DNS.
- If no address pool is configured, no addresses will be assigned.

4.3.2 DHCP Relay Agent

Working Principle

The destination IP address of DHCP request packets is 255.255.255.255, and these packets are forwarded within a subnet. To achieve IP address assignment across network segments, a DHCP relay agent is needed. The DHCP relay agent unicasts DHCP request packets to a DHCP server and forwards DHCP reply packets to a DCHP client. The DHCP relay agent serves as a repeater connecting a DHCP client and a DHCP server of different network segments by forwarding DHCP request packets and DHCP reply packets. The Client-Relay-Server mode achieves management of IP addresses across multiple network segments by only one DHCP server. See the following figure.

Figure 4-8 DHCP Relay Scenario



VLAN 10 and VLAN 20 correspond to the segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server with IP address 30.0.0.2 is in segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable DHCP Relay on a gateway and configure IP address 30.0.0.2 for the DHCP server.

↘ DHCP Relay Agent Information (Option 82)

As defined in RFC3046, an option can be added to indicate a DHCP client's network information when DHCP Relay is performed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The option is called Option 82. Currently, Ruijie devices support four schemes of relay agent information, which are described respectively as follows:

a) Relay agent information option82: This scheme serves without correlation with other protocol modules. A DHCP relay agent forms an Option 82 based on the physical port receiving DHCP request packets and the MAC address of the device. The option format is shown in the following figure.

Figure 4-9 Agent Circuit ID

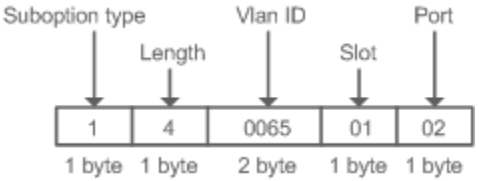
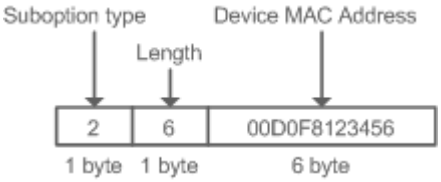


Figure 4-10 Agent Remote ID



DHCP Relay Check Server-ID

- In DHCP environment, multiple DHCP servers are deployed for a network, achieving server backup to ensure uninterrupted network operation. After this function is enabled, the DHCP request packet sent by a client contains a **server-id** option specifying a DHCP server. In alleviating the burden on servers in specific environments, you need to enable this function on a relay agent to send a packet to a specified DHCP server rather than all DHCP servers.

DHCP Relay suppression

After you configure the **ip DHCP Relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP request packets will be forwarded.

Related Configuration

Enabling DHCP Relay

- By default, DHCP Relay is disabled.
- You may run the **service dhcp** command to enable DHCP Relay.
- You need to enable DHCP Relay before it works.

Configuring IP Address for DHCP Server

- By default, no IP address is configured for a DHCP server.
- You may run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a layer-3 interface. A maximum of 20 IP addresses can be configured for a DHCP server.

Enabling DHCP Option 82

- By default, DHCP Option 82 is disabled.

- You may run the **ip dhcp relay information option82** command to enable DHCP Option 82.

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Enabling DHCP Relay Suppression

- By default, DHCP Relay suppression is disabled on all interfaces.
- You may run the **ip dhcp relay suppression** command to enable it on an interface.

4.3.3 DHCP Client

Working Principle

A DHCP client broadcasts a DHCP discover packet after entering the Init state. Then it may receive multiple DHCP offer packets. It chooses one of them and responds to the corresponding DHCP server. After that, it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling DHCP Client on Interface

- By default, DHCP Client is disabled.
- In interface configuration mode, you may run the **ip address dhcp** command to enable DHCP Client.
- You need to enable DHCP Client to enable DHCP service.
- The configuration takes effect on a layer-3 interface, for example, an SVI or a routed port.

4.3.4 AM Rule

Working Principle

An AM rule defines the range of IP addresses assigned to DHCP clients in different VLANs and ports. It can be used to quickly identify the VLAN and port of a faulty DHCP client and effectively assign addresses. After an AM rule is configured, all DHCP clients from the set VLAN and ports may obtain IP addresses. If no AM rule is configured, there are two following cases: If a default AM rule is configured, the client obtains an IP address from the default range; if no default AM rule is configured, the client cannot obtain an IP address.

Related Configuration

Configuring AM Rule in Global Configuration Mode

- In global configuration mode, run the **address-manage** command to enter AM rule configuration mode.
- Run the **match ip default** command to configure a default AM rule.
- Run the **match ip** command to configure an AM rule based on VLAN & port or port.

4.4 Configuration

Configuring DHCP Server

Configuration	Description and Command	
Configuring Dynamic IP Address	(Mandatory) It is used to enable DHCP Server to achieve dynamic IP address assignment.	
	service dhcp	Enables DHCP Server.
	ip dhcp pool	Configures an address pool.
	network	Configures the network number and subnet mask of a DHCP address pool.
	(Optional) It is used to configure the properties of an address pool.	
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address
	bootfile	Configures a boot file of a client.
	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
	update arp	Adds a trusted ARP while assigning addresses from a pool.
Configuring Static IP Address	(Optional) It is used to statically assign an IP address to a client.	
	ip dhcp pool	Configures an address pool name and enters address pool configuration mode.
	host	Configures the IP address and subnet mask of a client host.
	hardware-address	Configures a client hardware address.
	client-identifier	Configures a unique client identifier.
	client-name	Configures a client name.
Configuring Global Properties of DHCP Server	(Optional) It is used to configure the properties of a DHCP server.	
	ip dhcp excluded-address	Configures an excluded IP address.
	ip dhcp force-send-nak	Configures Compulsory NAK reply by a DHCP server.

Configuration	Description and Command	
	ip dhcp monitor-vrrp-state	Configures VRRP status monitoring.
	ip dhcp ping packets	Configures ping times.
	ip dhcp ping timeout	Configures a ping timeout.
	ip dhcp refresh arp	Configures a DHCP server to refresh trusted ARPs.
	ip dhcp server arp-detect	Configures a DHCP server to detect user offline.
	ip dhcp server detect	Configures pseudo server detection.
Configuring AM Rule for DHCP Server	(Optional) It is used to configure the AM rule of a DHCP server.	
	address-manage	Enters AM configuration mode.
	match ip default	Configures a default AM rule.
	match ip	Configures AM rule based on VLAN/VLAN and port.

Configuring DHCP Relay

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	(Mandatory) It is used to enable DHCP Relay.	
	service dhcp	Enables DHCP Relay.
	ip helper-address	Configures an IP Address of a DHCP Server.
Configuring DHCP Relay Option 82	(Optional) It is used to assign IP addresses of different privileges to clients in combination with the information of a physical port. This function cannot be used together with the **dhcp option dot1x** command.	
	ip dhcp relay information option82	Enables DHCP option82.
Configuring DHCP Relay Check Server-ID	(Optional) It is used to enable a DHCP Relay agent to send DHCP request packets only to a specified server.	
	ip dhcp relay check server-id	Enables a DHCP Relay agent to send DHCP request packets only to a specified server
Configuring DHCP Relay Suppression	(Optional) It is used to shield DHCP request packets on an interface.	
	ip dhcp relay suppression	Enables DHCP Relay Suppression.

Configuring DHCP Client

Configuration	Description and Command	
Configuring DHCP Client	(Mandatory) It is used to enable DHCP Client.	
	ip address dhcp	Enables an Ethernet interface, a PPP/HDLC-encapsulated or FR-encapsulated interface to obtain IP addresses through DHCP.

4.4.1 Configuring Dynamic IP Address

Configuration Effect

Provide all DHCP clients with DHCP service including assigning IP addresses and gateways.

Notes

A DHCP server and a DHCP relay share the **service dhcp** command, but a device cannot function as a DHCP server and relay at the same time. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuration Steps

Enabling DHCP Server

- Mandatory. It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

Configuring Address Pool

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

- Mandatory. It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

Configuring Default Gateway of Client

- Optional. It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

Configuring Address Lease

- Optional. It is used to configure an IP address lease, which is 24h by default.
- Run the **lease** command in DHCP address pool configuration mode.

Configuring TFTP Server Address

- Optional. It is used to configure a TFTP server address.
- Run the **next-server** command in DHCP address pool configuration mode.

Configuring Domain Name of Client

- Optional. It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring DNS

- Optional. It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring NetBIOS WINS Server

- Optional. It is used to configure a NetBIOS WINS server address.
- Run the **netbios-name-server** command in DHCP address pool configuration mode.

Configuring NetBIOS Node Type on Client

- Optional. It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring Alarm Threshold of Address Pool

- Optional. It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be printed.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring User-Defined Option

- Optional. It is used to configure user-defined options.
- Run the **option** command in DHCP address pool configuration mode.

Enabling or Disabling Address Pool

- Optional. It is used to enable or disable an address pool. It is enabled by default.
- Run the **pool-status** command in DHCP address pool configuration mode.

Adding Trusted ARP

- Optional. It is used to add a trusted ARP while assigning an IP address. It is disabled by default.
- Run the **update arp** command in DHCP address pool configuration mode.

Verification

Connect a DHCP client and a DHCP server.

- Check whether the client obtains configurations on the server.

Related Commands

Enabling DHCP Server

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable DHCP Server and DHCP Relay. A DHCP server and a DHCP relay share the **service dhcp** command. When a device is configured with a valid address pool, it acts as a server and forwards packets. Otherwise, it serves as a relay agent.

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter DHCP address pool configuration mode.

Configuring Network Number and Subnet Mask of DHCP Address Pool

Command	**network** *network-number mask* [*low-ip-address high-ip-address*]
Parameter Description	*network-number:* Indicates the network number of an IP address pool. *mask:* Indicates the subnet mask of an IP address pool. If no subnet mask is defined, the natural subnet mask is applied.
Command Mode	DHCP address pool configuration mode
Usage Guide	To configure dynamic address assignment, you need to configure a network number and subnet mask of an address pool to provide a DHCP server with a range of addresses. The IP addresses in a pool are assigned in order. If an address is assigned or exists in the target network segment, the next address will be checked until a valid address is assigned. Ruijie wireless products provide available network segments by specifying start and end addresses. The configuration is optional. If the start and end address are not specified, all IP addresses in the network segment are assignable. For Ruijie products, addresses are assigned based on the client's physical address and ID. Therefore, one client will not be assigned two leases from one address pool. In case of topological redundancy between a client and a server, address assignment may fail.

	To avoid such failures, a network administrator needs to prevent path redundancy in network construction, for example, by adjusting physical links or network paths.

Configuring Default Gateway of Client

Command	**default-router** *address* [*address2…address8*]
Parameter Description	*address*: Indicates the IP address of a default gateway. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 gateways can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure a default gateway of a client, and a server will push the gateway configuration to the client. The IP addresses of the default gateway and the client should be in a same network.

Configuring Address Lease

Command	**lease** {*days* [*hours]* [*minutes*] | **infinite**}
Parameter Description	*days:* Defines a lease in the unit of day. *hours:* (Optional) Defines a lease in the unit of hour. Please define *days* before *hours*. *minutes:* (Optional) Defines a lease in the unit of minute. Please define *days* and *hours* before *minutes*. **infinite:** Defines an unlimited lease.
Command Mode	DHCP address pool configuration mode
Usage Guide	The default lease of an IP address assigned by a DHCP server is 1 day. When a lease is expiring soon, a client needs to request a lease renewal. Otherwise the IP address cannot be used after the lease is expired.

Configures Boot File on Client

Command	**bootfile** *filename*
Parameter Description	*file-name*: Defines a boot file name.
Command Mode	DHCP address pool configuration mode
Usage Guide	A boot file is a bootable image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring Domain Name of Client

Command	**domain-name** *domain*
Parameter Description	*domain-name:* Defines a domain name of a DHCP client.
Command Mode	DHCP address pool configuration mode
Usage Guide	You may define a domain name for a client. When the client accesses network through the host name, the domain name will be added automatically to complete the host name.

Configuring DNS

Command	**dns-server** *ip-address* [*ip-address2…ip-address8*]
Parameter Description	*ip-address:* Defines an IP address of a DNS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 DNS servers can be configured. **use-dhcp-client** *interface-type interface-number:* A DHCP client learns its DNS server via RGOS software.
Command Mode	DHCP address pool configuration mode
Usage Guide	If a client accesses network resources through the domain name, you need to configure a DNS server to resolve the domain name.

Configuring NetBIOS WINS Server

Command	**netbios-name-server** *address* [*address2…address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. Configure at least one IP address. *ip-address2…ip-address8:* (Optional) A maximum of 8 WINS servers can be configured.
Command Mode	DHCP address pool configuration mode
Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetNBIOS name to an IP address. A WINS server is a Windows NT server. When a WINS server starts, it receives a registration request from a WINS client. When the client shuts down, it sends a name release message, so that the computers in the WINS database and on the network are consistent.

Configuring NetBIOS Node Type on Client

Command	**netbios-node-type** *type*
Parameter Description	type: Defines a NetBIOS node type with one of the following approaches. 1. A hexadecimal number, ranging from 0 to FF. Only followings values are available. ● b-node ● p-node ● m-node ● 8 for h-node 2. A character string. ● b-node for a broadcast node; ● p-node for a peer-to-peer node; ● m-node for a mixed node; ● h-node for a hybrid mode.
Command Mode	DHCP address pool configuration mode
Usage Guide	There are four types of NetBIOS nodes of a Microsoft DHCP client. 1) A broadcast node. For such a node, NetBIOS name resolution is requested through broadcast.2) A peer-to-peer node. The client sends a resolution request to the WINS server. 3) A mixed node. The client broadcasts a resolution request and sends the resolution request to the WINS server.. 4) A hybrid node. The client sends a resolution request to

	the WINS server. If no reply is received, the client will broadcast the resolution request. By default, a Microsoft operating system is a broadcast or hybrid node. If no WINS server is configured, it is a broadcast node. Otherwise, it is a hybrid node.

Configuring User-Defined Option

Command	**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }
Parameter Description	*code:* Defines a DHCP option code. **ascii** *string:* Defines an ASCII character string. **hex** *string:* Defines a hexadecimal character string. **ip** *ip-address:* Defines an IP address.
Command Mode	DHCP address pool configuration mode
Usage Guide	The DHCP allows transmitting configuration information to a host via a TCP/IP network. DHCP packets contain the option field of definable content. A DHCP client should be able to receive a DHCP packet carrying at least 312 bytes option. Besides, the fixed data field in a DHCP packet is also called an option. In a WLAN, a DHCP client on an AP dynamically requests the IP address of an AC. You may configure on a DHCP server the **option** command specifying the AC address.

Enabling or Disabling Address Pool

Command	**pool-status** {**enable | disable**}
Parameter Description	**enable***:* Enables an address pool. **disable***:* Disable an address pool. It is enabled by default.
Command Mode	DHCP address pool configuration mode
Usage Guide	A Ruijie wireless product provides a command for you to enable/disable a DHCP address pool.

Adding Trusted ARP

Command	**update arp**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	After configuration, a trusted ARP is added when an address is assigned from a pool. A trusted ARP prevents ARP spoofing.

Configuration Example

Configuring Address Pool

Configuration	● Define an address pool net172.

Steps	● The network segment is 172.16.1.0/24. ● The default gateway is 172.16.1.254. ● The address lease is 1 day. ● xcluded addresses range from 172.16.1.2 to 172.16.1.100.
	Ruijie(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100 Ruijie(dhcp-config)# ip dhcp pool net172 Ruijie(dhcp-config)# network 172.16.1.0 255.255.255.0 Ruijie(dhcp-config)# default-router 172.16.1.254 Ruijie(dhcp-config)# lease 1
Verification	● Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip dhcp ip dhcp excluded-address 172.16.1.2 172.16.1.100 ip dhcp pool net172 network 172.16.1.0 255.255.255.0default-router 172.16.1.254 lease 1

4.4.2 Configuring Static IP Address

Configuration Effect

Assign specific IP addresses and push configuration to specific DHCP clients.

Notes

N/A

Configuration Steps

Configuring Address Pool Name and Entering Address Pool Configuration Mode

- Mandatory. It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

Configuring IP Address and Subnet Mask of Client

- Mandatory. It is used to configure a static IP address and a subnet mask.
- Run the **host** command in DHCP address pool configuration mode.

Configuring Hardware Address of Client

- Optional. It is used to configure a MAC address.

- Run the **hardware** command in DHCP address pool configuration mode.

Configures Unique Client Identifier

- Optional. It is used to configure a static user identifier (UID).
- Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring Client Name

- Optional. It is used to configure a static client name.
- Run the **host-name** command in DHCP address pool configuration mode.

Verification

Check whether the client obtains the IP address when it is online.

Related Commands

Configuring Address Pool

Command	**ip dhcp pool** *dhcp-pool*
Parameter Description	*pool-name*: Indicates the name of an address pool.
Command Mode	Global configuration mode
Usage Guide	Before assigning an IP address to a client, you need to configure an address pool name and enter address pool configuration mode.

Manual IP Address Binding

Command	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Parameter Description	*ip-address:* Defines the IP address of a DHCP client. *netmask:* Defines the subnet mask of a DHCP client. *unique-identifier:* Defines the hardware address (for example, aabb.bbbb.bb88) and identifier (for example, 01aa.bbbb.bbbb.88) of a DHCP client. *name:* (Optional) It defines a client name using ASCII characters. The name excludes a domain name. For example, name a host **mary** rather than **mary.rg.com**.
Command Mode	DHCP address pool configuration mode
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two kind of address binding. 1) Manual binding. Manual binding can be deemed as a special DHCP address pool with only one address. 2) Dynamic binding. A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP request, creating mapping between the IP address and the client's MAC address.

	To configure manual binding, you need to define a host pool and then specify a DHCP client's IP address and hardware address or identifier. A hardware address is a MAC address. A client identifier includes a network medium type and a MAC address. A Microsoft client is usually identified by a client identifier rather than a MAC address. For the codes of medium types, refer to the *Address Resolution Protocol Parameters* section in the RFC 1700. The Ethernet type is **01**.

Configuration Example

Dynamic IP Address Pool

Configuration Steps	● Configure address pool VLAN 1 with IP address 20.1.1.0 and subnet mask 255.255.255.0. ● The default gateway is 20.1.1.1. ● The lease time is 1 day.
	Ruijie(config)# ip dhcp pool vlan1 Ruijie(dhcp-config)# network 20.1.1.0 255.255.255.0 Ruijie(dhcp-config)# default-router 20.1.1.1 Ruijie(dhcp-config)# lease 1 0 0
Verification	● Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip dhcp ip dhcp pool vlan1 network 20.1.1.0 255.255.255.0 default-router 20.1.1.1 lease 1 0 0

Manual Binding

Configuration Steps	● The host address is 172.16.1.101 and the subnet mask is 255.255.255.0. ● The host name is Billy.rg.com. ● The default gateway is 172.16.1.254. ● The MAC address is 00d0.df34.32a3.
	Ruijie(config)# ip dhcp pool Billy Ruijie(dhcp-config)# host 172.16.1.101 255.255.255.0 Ruijie(dhcp-config)# client-name Billy Ruijie(dhcp-config)# hardware-address 00d0.df34.32a3 Ethernet Ruijie(dhcp-config)# default-router 172.16.1.254
Verification	● Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip dhcp

	ip dhcp pool Billy host 172.16.1.101 255.255.255.0 client-name Billy hardware-address 00d0.df34.32a3 Ethernet default-router 172.16.1.254

4.4.3 Configuring AM Rule for DHCP Server

Configuration Effect

Assign IP addresses according to an AM rule based on a port and a VLAN.

Notes

Ruijie products support AM rule configuration on Ethernet, GB, FR, PPP and HDLC interfaces.

Configuration Steps

Configuring Address Management

- Mandatory. Enter address management mode.
- Run the **address-manage** command in address management configuration mode.

Verification

Check whether clients in different VLANs and ports obtain the valid IP addresses.

Related Commands

Configuring Default Range

Command	**match ip default** *ip-address netmask*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask.
Command Mode	Address management mode
Usage Guide	After configuration, all DHCP clients are assigned IP addresses from the default range based on the VLAN and port. If this command is not configured, IP addresses will be assigned through the regular process.

Assigning Dynamic IP Address Based on VLAN and Port

Command	**match ip** *ip-address netmask interface* [**add**/**remove**] **vlan** *vlan-list*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask. *interface:* Defines an interface name. *add/remove:* Adds or deletes a specific VLAN.

	vlan-list: Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	After configuration, DHCP clients are assigned IP addresses from the default address range based on the VLAN and port.

Assigning Static IP Address Based on VLAN

Command	**match ip** *ip-address netmask* [**add**/**remove**] **vlan** *vlan-list*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask. *add/remove:* Adds or deletes a specific VLAN. *vlan-list:* Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	In a Super VLAN, a client may be assigned a fixed static address no matter which Super VLAN the client resides in. You do not need to configure an AM rule for this IP address based on all sub-VLANs and ports, but only configure an AM rule based on the VLAN. This rule takes effect for only static address assignment.

Configuration Example

Configuring AM Rule

Configuration Steps	● Configure a default rule. ● Configure a rule based on a specific VLAN, port and address range. ● Configure a rule based on a specific VLAN and address range.
	Ruijie(config)# address-manage Ruijie(config-address-manage)# match ip default 172.50.128.0 255.255.128.0 Ruijie(config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 Ruijie(config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006
Verification	● 1: Run the **show run** command to display the configuration.
	address-manage match ip default 172.50.128.0 255.255.128.0 match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005 match ip 10.1.6.0 255.255.255.0 vlan 1006

4.4.4 Configuring Global Properties of DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and compulsory NAK.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Steps

Configuring Excluded IP Address

- Optional. Configure some addresses or address ranges as unavailable.
- Run the **ip dhcp excluded-address** command in global configuration mode.

Configuring Compulsory NAK Reply

- Optional. A server replies to a wrong address request with a NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

Configuring VRRP Status Monitoring

- Optional. After configuration, DHCP packets are processed by the Master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring Ping Times

- Optional. Check the address reachability with the **ping** command. The default is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional. Check the address reachability with the **ping** command. The default is 500 ms.
- Run the **ip dhcp ping timeout** command in global configuration mode.

Refreshing Trusted ARP

- Configure a DHCP server to refresh trusted ARPs according to the addresses assigned from an address pool configured with the **update arp** command.
- Run the **ip dhcp refresh arp** command in global configuration mode.

Detecting User Offline Detection

- Configure a DHCP server to detect whether the client is offline or not. If a client does not get online after being offline for a period, the address assigned to the client will be retrieved.
- Run the **ip dhcp server arp-detect** command in global configuration mode.

Configuring Pseudo Server Detection

- Optional. Enable this function to log a pseudo server.
- Run the **ip dhcp server detect** command in global configuration mode.

Verification

Run the **dhcp-server** command, and check the configuration during address assignment.

Related Commands

Configuring Excluded IP Address

Command	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates a start IP address. *high-ip-address:* Indicates an end IP address.
Command Mode	Global configuration mode
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

Configuring Compulsory NAK Reply

Command	**ip dhcp force-send-nak**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In a WLAN, a DHCP client often moves from one network to another. When a DHCP server receives a lease renewal request from a client but finds that the client crosses the network segment or that the lease is expired, it replies with a NAK packet to require the client to obtain an IP address again. This prevents the client from sending request packets continually before obtaining an IP address again after timeout. The server sends a NAK packet only when it finds the client's lease record. When a DHCP client crosses the network, a DHCP server cannot find lease record of the client and will not reply with a NAK packet. The client sends request packets continually before obtaining an IP address again after timeout. Consequently, it takes a long to obtain an IP address. This also occurs when a DHCP server loses a lease after restart and a client requests lease renewal. In this case, you may configure a command to force the DHCP server to reply with a NAK packet even though it cannot find the lease record so that the client may obtain an IP address rapidly. Please note that the command is disabled by default. To enable it, only one DHCP server can be configured in a broadcast domain.

Configuring Ping Times

Command	**ip dhcp ping packets** [*number*]
Parameter Description	*number:* (Optional) Ranges from 0 to 10. 0 indicates the ping function is disabled. The default is two pings.
Command Mode	Global configuration mode
Usage Guide	By default, when a DHCP server assigns an IP address from a pool, it runs the **Ping** command twice (one packet per time). If there is no reply, the server takes the address as idle and assigns it to a client. If there is a reply, the server takes the address as occupied and assigns another address.

Configuring Ping Timeout

Command	**ip dhcp ping timeout** *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that it takes for a DHCP server to wait for a ping reply. The value ranges from 100 ms to 10,000 ms.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no Ping reply within 500 ms, the IP address is available. You may adjust the ping timeout to change the time for a server to wait for a reply.

Refreshing Trusted ARP

Command	**ip dhcp refresh arp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, if an address pool is configured with the **update arp** command, a DHCP server will refresh trusted ARPs while assigning an IP address from the address pool. If a client clears the trusted ARPs, the server will not reassign them. After configuration, a DHCP server may refresh trusted ARPs according to addresses assigned from an address pool configured with **update arp**.

Configuring ARP-Based Offline Detection

Command	**ip dhcp server arp-detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, DHCP server does not detect whether a client is offline or not based on ARP. After configuration, a DHCP server may perform the detection. If a client does not get online again after a period (5 minutes by default), a DHCP server retrieves the address assigned to the client.

Configuring Pseudo Server Detection

Command	ip dhcp server detect
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, pseudo server detection is disabled on a DHCP server. Run this command to enable pseudo server detection.

Configuration Example

Configuring Ping

Configuration Steps	● Set ping times to 5. ● Set ping timeout to 800ms.
	Ruijie(config)# ip dhcp ping packet 5 Ruijie(config)# ip dhcp ping timeout 800
Verification	● Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip dhcp ip dhcp ping packet 5 ip dhcp ping timeout 800

Configuring Excluded IP Address

Configuration Steps	● Configure the excluded IP address from 192.168.0.0 to 192.168.255.255.
	Ruijie(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
Verification	● Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip dhcp ip dhcp excluded-address 192.168.0.0 192.168.255.255

4.4.5 Configuring Basic DHCP Relay Functions

Configuration Effect

- Deploy dynamic IP management in Client–Relay–Server mode to achieve communication between a DHCP client and a DHCP server, which are in different network segments.

Notes

- To enable DHCP Relay, you need to configure IPv4 unicast routing in a network.

Configuration Steps

Enabling DHCP Relay

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

Configuring IP Address for DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through DHCP Relay.

Related Commands

Enabling DHCP Relay

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring IP Address for DHCP Server

Command	**ip helper-address { cycle-mode |** *A.B.C.D* **}**
Parameter Description	*cycle-mode*: Indicates that DHCP request packets are forwarded to all DHCP servers. *A.B.C.D*: Indicates the IP address of a server.
Command Mode	Global configuration mode
Usage Guide	

Configuration Example

Configuring DHCP Relay in Wired Connection

Scenario **Figure 4-11**	

Configuration Steps	● Enable a client with DHCP to obtain an IP address. ● Enable the DHCP Relay function on a DHCP relay agent. ● Configure DHCP Server.
A	Enable a client with DHCP to obtain an IP address.
B	Enable DHCP Relay. Ruijie(config)# service dhcp Configure a global IP address of a DHCP server. Ruijie(config)# ip helper-address 172.2.2.1 Configure an IP address for the port connected to the client. Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if)# ip address 192.1.1.1 255.255.255.0 Configure an IP address for the port connected to the server. Ruijie(config)# interface gigabitEthernet 0/2 Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
C	Enable DHCP Server. Ruijie(config)# service dhcp Configure an address pool. Ruijie(config)# ip dhcp pool relay Ruijie (dhcp-config)#network 192.1.1.0 255.255.255.0 Ruijie (dhcp-config)#default-router 192.1.1.1 Configure an IP address for the port connected to the relay agent. Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
Verification	Check whether the client obtains an IP address. ● Check whether the client obtains an IP address. ● Check the DHCP Relay configuration.
A	The user device obtains an IP address.
B	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration. Ruijie# show running-config service dhcp ip helper-address 172.2.2.1 !

	interface GigabitEthernet 0/1 ip address 192.1.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 ip address 172.2.2.2 255.255.255.0 !

Common Errors

- IPv4 unicast routing configuration is incorrect.
- DHCP Relay is disabled.
- No routing between DHCP relay agent and DHCP server is configured.
- No IP address is configured for the DHCP server.

4.4.6 Configuring DHCP Relay Option 82

Configuration Effect

- Through a DHCP relay agent, a server may assign IP addresses of different privileges to the clients more accurately based on the option information.

Notes

- You need to enable the DHCP Relay function.

Configuration Steps

↘ Enabling Basic DHCP Relay Functions

- Mandatory.
- Unless otherwise specified, you need to enable DHCP Relay on a device.

↘ Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- You may run the **ip dhcp relay information option82** command to enable or disable DHCP Option 82.

Verification

- Check whether the client obtains an IP address based on Option 82.

Related Commands

↘ Enabling DHCP Option 82

Command	**ip dhcp relay information option82**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling DHCP Option 82

Configuration Steps	● Enable DHCP Option 82.
	Ruijie(config)# ip dhcp relay information option82
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Ruijie#show ru | incl ip dhcp relay ip dhcp relay information option82

Common Errors

- Basic DHCP Relay functions are not configured.

4.4.7 Configuring DHCP Relay Check Server-ID

Configuration Effect

- After you configure the **ip dhcp relay check server-id**, a DHCP Relay agent will forward DHCP request packets only to the server specified by the **option server-id** command. Otherwise, they are forwarded to all DHCP servers.

Notes

- You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Check Server-ID

- By default, DHCP Relay check server-id is disabled.
- You may run the **ip dhcp relay check server-id** command to enable DHCP Relay check server-id.

Verification

Check whether a DHCP Relay agent sends DHCP request packets only to the server specified by the **option server-id** command.

Related Commands

Configuring DHCP Relay Check Server-ID

Command	**ip dhcp relay check server-id**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Check Server-ID

Configuration Steps	● Enable DHCP Relay.Omitted. ● Enable **DHCP Relay check server-id** on an interface.
	Ruijie# configure terminal Ruijie(config)# ip dhcp relay check server-id
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Ruijie# show running-config | include check server-id ip dhcp relay check server-id Ruijie#

Common Errors

- Basic DHCP Relay functions are not configured.

4.4.8 Configuring DHCP Relay Suppression

Configuration Effect

- After you configure the **ip DHCP Relay suppression** command on an interface, DHCP request packets received on the interface will be filtered, and the other DHCP requests will be forwarded.

Notes

- You need to enable basic DHCP Relay functions.

Configuration Steps

Enabling DHCP Relay Suppression

By default, DHCP Relay suppression is disabled on all interfaces.

- You may run the **ip dhcp relay suppression** command to enable DHCP Relay suppression.

Verification

- Check whether the DHCP request packets received on the interface are filtered.

Related Commands

Configuring DHCP Relay Suppression

Command	**ip dhcp relay suppression**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring DHCP Relay Suppression

Configuration Steps	● Configure basic DHCP Relay functions. ● Configure DHCP Relay suppression on an interface.
	Ruijie# configure terminal Ruijie(config)# interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression Ruijie(config-if-GigabitEthernet 0/1)#end Ruijie#
Verification	After login to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display DHCP Relay configuration.
	Ruijie# show running-config | include relay suppression ip dhcp relay suppression Ruijie#

Common Errors

Basic DHCP Relay functions are not configured.

4.4.9 Configuring DHCP Client

Configuration Effect

Enable DHCP Client on a device so that it obtains IP addresses and configurations dynamically.

Notes

Ruijie products support DHCP Client configuration on Ethernet, FR, PPP and HDLC interfaces.

Configuration Steps

Run the **ip address dhcp** command on an interface.

Verification

Check whether the interface obtains an IP address.

Related Commands

↘ Configuring DHCP Client

Command	**ip address dhcp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	● Ruijie products support dynamic IP address obtainment by an Ethernet interface. ● Ruijie products support dynamic IP address obtainment by a PPP-encapsulated interface. ● Ruijie products support dynamic IP address obtainment by an FR-encapsulated interface. ● Ruijie products support dynamic IP address obtainment by an HDLC-encapsulated interface.

Configuration Example

↘ Configuring DHCP Client

Configuration Steps	● 1: Enable port FastEthernet 0/0 with DHCP to obtain an IP address.
	Ruijie(config)# interface FastEthernet0/0 Ruijie(config-if-FastEthernet 0/0)#ip address dhcp
Verification	● 1: Run the **show run** command to display the configuration.
	Ruijie(config)#show run | begin ip address dhcp ip address dhcp

4.5 Monitoring

Clearing

Running the clear commands may lose vital information and interrupt services.

Description	Command
Clears DHCP address binding.	**clear ip dhcp binding** { *address* | *}
Clears DHCP address conflict.	**clear ip dhcp conflict** { *address* | *}
Clears statistics of a DHCP server.	**clear ip dhcp server statistics**
Clears statistics of a DHCP relay.	**clear ip dhcp relay statistics**
Clears statistics of DHCP server performance.	**clear ip dhcp server rate**
Clears information of a DHCP pseudo server.	**clear ip dhcp server detect**

Displaying

Description	Command
Displays DHCP lease.	**show dhcp lease**
Displays DHCP sockets.	**show ip dhcp socket**
Displays assigned IP addresses.	**show ip dhcp binding**
Displays created address pools.	**show ip dhcp pool**
Displays statistics of DHCP Server.	**show ip dhcp server statistic**
Displays statistics of DHCP Relay.	**show ip dhcp relay statistic**
Displays conflicted addresses.	**show ip dhcp conflict**
Displays the DHCP pseudo server.	**show ip dhcp server detect**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCP agent.	**debug ip dhcp server agent**
Debugs DHCP hot backup.	**debug ip dhcp server ha**
Debugs DHCP address pools.	**debug ip dhcp server pool**
Debugs DHCP VRRP.	**debug ip dhcp server vrrp**
Debugs all DHCP servers.	**debug ip dhcp server all**
Debugs DHCP packets.	**debug ip dhcp client**
Debugs DHCP Relay events.	**debug ip dhcp relay**

5 Configuring DHCPv6

5.1 Overview

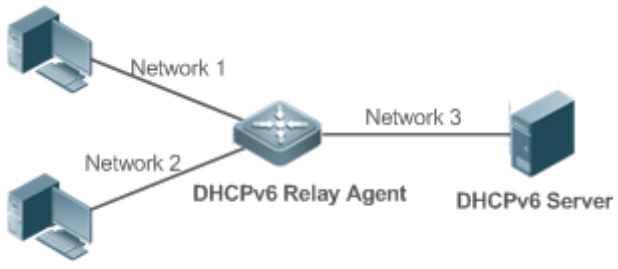
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows a DHCP server to transfer configurations (such as IPv6 addresses) to IPv6 nodes.

As compared with other IPv6 address allocation methods, such as manual configuration and stateless automatic address configuration, DHCPv6 provides the address allocation, prefix delegation, and configuration parameter allocation.

- DHCPv6 is a stateful protocol for automatically configuring addresses and flexibly adding and reusing network addresses, which can record allocated addresses and enhance network manageability.
- By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.
- The DHCPv6 configuration parameter allocation solves the problem that parameters cannot be obtained through a stateless automatic address configuration protocol and allocates DNS server addresses and domain names to hosts.
- DHCPv6 is a protocol based on the client/server model. A DHCPv6 client is used to obtain various configurations whereas a DHCPv6 server is used to provide various configurations. If the DHCPv6 client and DHCPv6 server are not on the same network link (the same network segment), they can interact with each other by using a DHCPv6 relay agent.

The DHCPv6 client usually discovers the DHCPv6 server by reserving multicast addresses within a link; therefore, the DHCPv6 client and DHCPv6 server must be able to directly communicate with each other, that is, they must be deployed within the same link. This may cause management inconvenience, economic waste (a DHCPv6 server is deployed for each subnet) and upgrade inconvenience. The DHCPv6 relay agent function can solve these problems by enabling a DHCPv6 client to send packets to a DHCPv6 server on a different link. The DHCP relay agent is often deployed within the link where a DHCPv6 client resides and is used to relay interaction packets between the DHCPv6 client and DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 5-1



Protocols and Standards

- RFC3315: Dynamic Host Configuration Protocol for IPv6
- RFC3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6

- RFC3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC3736: Stateless DHCP Service for IPv6
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

5.2 Applications

Application	Description
Requesting/Allocating Addresses and Configuration Parameters	A DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.
Requesting/Allocating Prefixes	The DHCPv6 client requests a prefix from the DHCPv6 server. The DHCPv6 server allocates a prefix to the DHCPv6 client and then the DHCPv6 client configures IPv6 addresses by using this prefix.
Relay Service	The DHCPv6 relay is used to enable communication between the DHCPv6 client and DHCPv6 server on different links.

5.2.1 Requesting/Allocating Addresses and Configuration Parameters

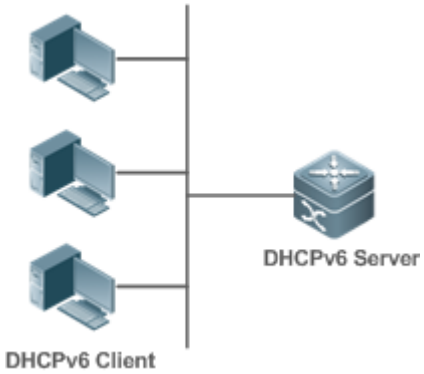
Scenario

In a subnet, a DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.

As shown in Figure 5-2:

- The DHCPv6 server is configured with IPv6 addresses, DNS servers, domain names and other configuration parameters to be allocated.
- A host works as a DHCPv6 client to request an IPv6 address from the DHCPv6 server. After receiving the request, the DHCPv6 server selects an available address and allocates the address to the host.
- The host can also request a DNS server, domain name and other configuration parameters from the DHCPv6 server.

Figure 5-2



Deployment

- Run the DHCPv6 client on a host in the subnet to obtain an IPv6 address and other parameters.
- Run the DHCPv6 server on a device and configure the IPv6 address and other parameters to allocate the IPv6 address and parameters.

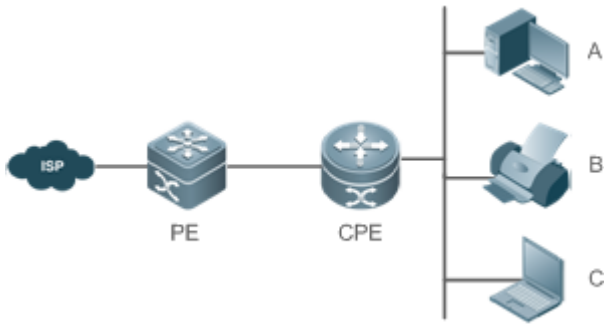
5.2.2 Requesting/Allocating Prefixes

Scenario

As shown in Figure 5-3, an uplink device (PE) allocates an IPv6 address prefix for a downlink device (CPE). The CPE generates a new address prefix for the internal subnet based on the obtained prefix. Hosts in the internal subnet of the CPE are configured with addresses through Router Advertisement (RA) by using the new address prefix.

- The PE provides the prefix delegation service as a DHCPv6 server.
- The CPE requests an address prefix from the PE as a DHCPv6 client. After obtaining the address prefix, the CPE generates a new address prefix for the internal subnet and sends an RA message to hosts in the internal subnet.
- The hosts in the internal subnet where CPE resides configure their addresses based on the RA message sent by the CPE.

Figure 5-3



Remarks	The Provider Edge (PE) works as a DHCPv6 server for providing prefixes and is also called a delegating router. The Customer Premises Equipment (CPE) works as a DHCPv6 client for requesting prefixes and is also called a requesting router. A, B and C are various hosts.

Deployment

- Run the DHCPv6 server on the PE to implement the prefix delegation service.
- Run the DHCPv6 client on the CPE to obtain address prefixes.
- Deploy IPv6 ND between the CPE and the hosts to configure the host addresses in the subnet through RA.

5.2.3 Relay Service

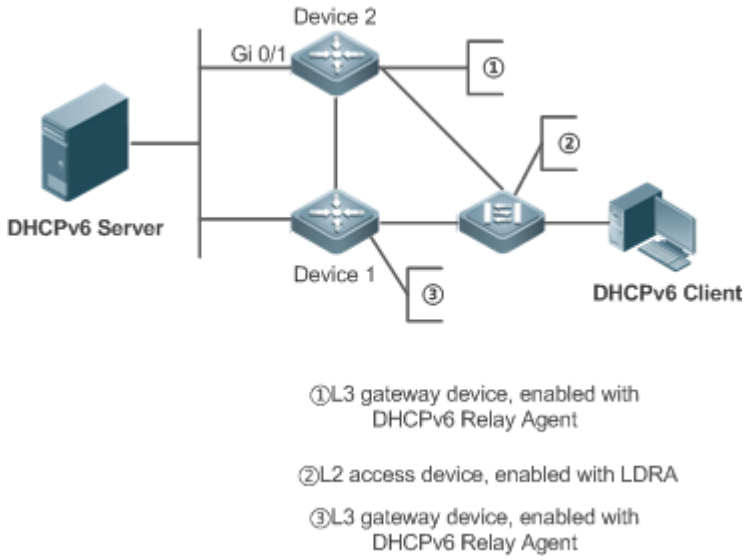
Scenario

The DHCPv6 relay agent provides the relay service for the DHCPv6 client ad DHCPv6 server on different links to enable communication between them.

As shown in Figure 5-4:

- Device 1 is enabled with the DHCPv6 relay agent and destined to 3001::2.
- Device 2 wants to forward packets to other servers through a next-level relay service. Enable the DHCPv6 relay agent on Device 2, set the destination address to FF02::1:2 (all servers and Relay multicast addresses) and specify the egress interface as the layer-3 interface gi 0/1.

Figure 5-4



Deployment

- Enable the DHCPv6 relay agent on device 1 and specify the address as 3000::1.
- Enable the DHCPv6 relay agent on device 2 and specify the address as FF02::1:2.

5.3 Features

Basic Concept

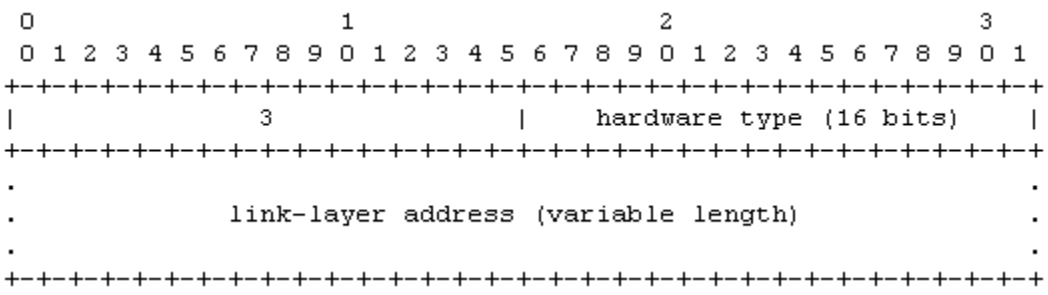
DUID

The DHCP Unique Identifier (DUID) identifies a DHCPv6 device. As defined in RFC3315, each DHCPv6 device (DHCPv6 client, relay or server) must have a DUID, which is used for mutual authentication during DHCPv6 message exchange.

RFC3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT).
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN).
- Link-Layer address (DUID-LL).

Ruijie DHCPv6 devices use DUID-LLs. The structure of a DUID-LL is as follows:



The values of *DUID-LL*, *Hardware type*, and *Link-layer address* are 0x0003, 0x0001 (indicating the Ethernet), and MAC address of a device respectively.

Identity Association (IA)

A DHCPv6 server allocates IAs to DHCPv6 clients. Each IA is uniquely identified by an identity association identifier (IAID). IAIDs are generated by DHCPv6 clients. A one-to-one mapping is established between IAs and clients. An IA may contain several addresses, which can be allocated by the client to other interfaces. An IA may contain one of the following types of addresses:

- Non-temporary Addresses (NAs), namely, globally unique addresses.
- Temporary Addresses (TAs), which are hardly used.
- Prefix Delegation (PD).

Based on the address type, IAs are classified into IA_NA, IA_TA, and IA_PD (three IA-Types). Ruijie DHCPv6 servers support only IA_NA and IA_PD.

Binding

A DHCPv6 binding is a manageable address information structure. The address binding data on a DHCPv6 server records the IA and other configurations of every client. A client can request multiple bindings. The address binding data on a server is present in the form of an address binding table with DUID, IA-Type and IAID as the indexes. A binding containing configurations uses DUID as the index.

DHCPv6 Conflict

When an address allocated by a DHCPv6 client is in conflict, the client sends a Decline packet to notify the DHCPv6 server that the address is rebound. Then, the server adds the address to the address conflict queue. The server will not allocate the addresses in the address conflict queue. The server supports viewing and clearing of address information in the address conflict queue.

Packet Type

RFC3315 stipulates that DHCPv6 uses UDP ports 546 and 547 for packet exchange. Specifically, a DHCPv6 client uses port 546 for receiving packets, while a DHCPv6 server and DHCPv6 relay agent use port 547 for receiving packets. RFC3315 defines the following types of packets that can be exchanged among the DHCPv6 server, client, and relay agent:

- Packets that may be sent by a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-request.
- Packets that may be sent by a DHCPv6 server to a DHCPv6 client include Advertise, Reply, and Reconfigure.
- Packets that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-forward.
- Packets that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-reply.

Ruijie DHCPv6 servers do not support the Reconfigure packet.

Ruijie DHCPv6 clients do not support the Confirm and Reconfigure packets.

Overview

Feature	Description
Requesting/Allocating Addresses	Dynamically obtains/allocates IPv6 addresses in a network in the client/server mode.
Requesting/Allocating Prefixes	Dynamically obtains/allocates IPv6 prefixes in a network in the client/server mode.
Stateless Service	Provides stateless configuration service for hosts in a network.
Relay Service	Provides the DHCPv6 server service for hosts in different networks by using the relay service.

5.3.1 Requesting/Allocating Addresses

A DHCPv6 client can request IPv6 addresses from a DHCPv6 server.

After being configured with available addresses, a DHCPv6 server can provide IPv6 addresses to hosts in the network, record the allocated addresses and improve the network manageability.

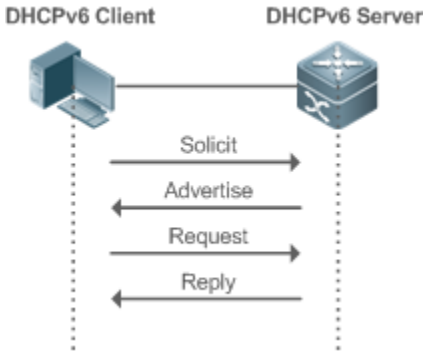
Working Principle

Network hosts serve as DHCPv6 clients and DHCPv6 servers to implement address allocation, update, confirmation, release and other operations through message exchange.

Four-Message Exchange

Figure 5-5 shows the four-message exchange process.

Figure 5-5

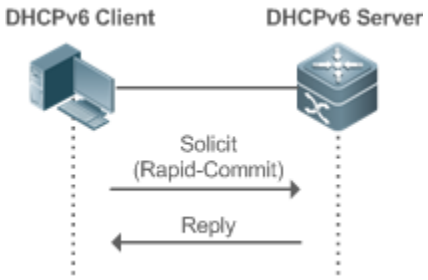


- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. All DHCPv6 servers or DHCPv6 relay agents within the link will receive the Solicit message.
- After receiving the Solicit message, a DHCPv6 server will send an Advertise message in the unicast mode if it can provide the information requested in the Solicit message. The Advertise message includes the address, prefix and configuration parameters.
- The DHCPv6 client may receive the Advertise message from multiple DHCPv6 servers. After selecting the most suitable DHCPv6 server, the DHCPv6 client sends a Request message whose destination address is FF02::1:2 and destination port number is 547 to request address, prefix and configuration parameter allocation.
- After receiving the Request message, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters that the DHCPv6 server will allocate to the DHCPv6 client. The DHCPv6 client obtains address, prefix or configuration parameters based on the information in the Reply message.

Two-Message Exchange

Two-message exchange can be used to complete address, prefix and parameter configuration for DHCPv6 clients more quickly.

Figure 5-6



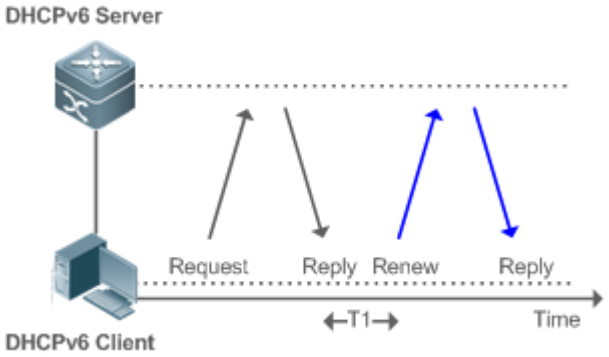
- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix and configuration parameter allocation. The Solicit message contains Rapid Commit.
- If a DHCPv6 server supports the Rapid Commit option, the DHCPv6 server creates a binding locally and sends a Reply message in the unicast mode. The Reply message includes the address, prefix and configuration parameters to be

allocated to the DHCPv6 client. The DHCPv6 client completes configuration based on the information in the Reply message.

Update and Rebinding

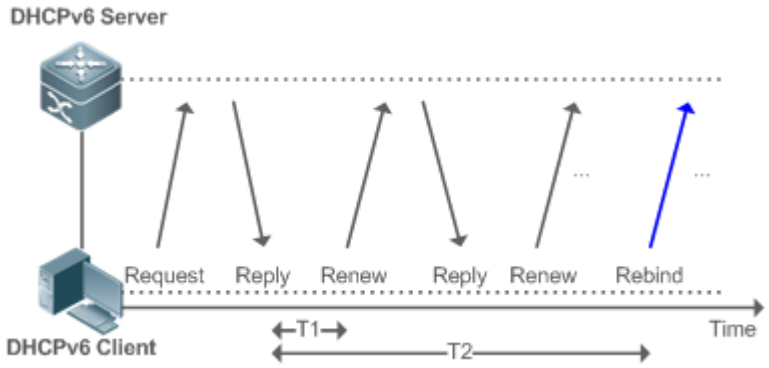
The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the message sent to the DHCPv6 client.

Figure 5-7



- The DHCPv6 client will send a Renew multicast message to the DHCPv6 server for updating the address and prefix after T1 seconds. The Renew message contains the DUID of the DHCPv6 server and the IA information to be updated.
- After receiving the Renew message, the DHCPv6 server checks whether the DUID value in the Renew message is equal to the DUID value of the local device. If yes, the DHCPv6 server updates the local binding and sends a Reply message in the unicast mode. The Reply message contains the new T1 and other parameter s.

Figure 5-8

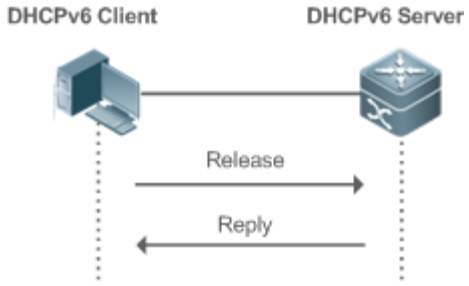


- If no response is received after the DHCPv6 client sends a Renew message to the DHCPv6 server, the DHCPv6 client will send a Rebind multicast message to the DHCPv6 server for rebinding the address and prefix after T2 expires.
- After receiving the Rebind message, the DHCPv6 server (perhaps a new DHCPv6 server) sends a Reply message according to the content of the Rebind message.

Release

If a DHCPv6 client needs to release an address or a prefix, the DHCPv6 client needs to send a Release message to a DHCPv6 server to notify the DHCPv6 server of the released addresses or prefixes. In this way, the DHCPv6 server can allocate these addresses and prefixes to other DHCPv6 clients.

Figure 5-9



- After receiving the Release message, the DHCPv6 server removes the corresponding bindings based on the addresses or prefixes in the Release message, and sends a Reply message carrying the state option to the DHCPv6 client.

Confirmation

After moving to a new link (for example, after restart), a DHCPv6 client will send a Confirm message to the DHCPv6 server on the new link to check whether the original addresses are still available.

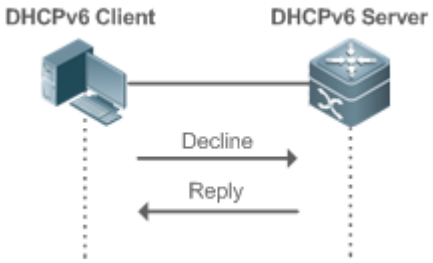
Figure 5-10

- After receiving the Confirm message, the DHCPv6 server performs confirmation based on the address information in the Confirm message, and sends a Reply message carrying the state option to the DHCPv6 client. If the confirmation fails, the DHCPv6 client may initiate a new address allocation request.

DHCPv6 Conflict

If the DHCPv6 client finds that the allocated addresses have been used on the link after address allocation is completed, the DHCPv6 client sends a Decline message to notify the DHCPv6 server of the address conflict.

Figure 5-11



- The DHCPv6 client includes the IA information of the conflicted addresses in the Decline message.
- After receiving the Decline message, the DHCPv6 server marks the addresses in the Decline message as "declined" and will not allocate these addresses . Then, the DHCPv6 server sends a Reply message carrying the state option to the DHCPv6 client. You can manually clear addresses marked as "declined" to facilitate re-allocation.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable the DHCPv6 server function for the interface.

The DHCPv6 server function must be enabled on a layer-3 interface.

Allocating Addresses Through the DHCPv6 Server

- By default, the DHCPv6 server has no configuration pool and is not configured with addresses to be allocated.
- You can run the **ipv6 dhcp pool** command to create a configuration pool.
- You can run the **iana-address** command to configure addresses to be allocated and the **preferred lifetime** and **valid lifetime** values.

Clearing Conflicted Addresses Through the DHCPv6 Server

- By default, the DHCPv6 server does not clear conflicted addresses that are detected.
- You can run the **clear ipv6 dhcp conflict** command to clear conflicted addresses so that these addresses can be reused.

Enabling the DHCPv6 Client Address Request Function on an Interface

- By default, an interface is not enabled with the DHCPv6 client address request function.
- You can run the **ipv6 dhcp client ia** command to enable the DHCPv6 client address request function for the interface.

The DHCPv6 client address request function is effective only on a layer-3 interface.

5.3.2 Requesting/Allocating Prefixes

Configure available prefixes on the DHCPv6 server. By using the prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and flexible control of station address space.

Working Principle

Downlink network devices serve as DHCPv6 clients to exchange messages with the DHCPv6 server to implement address allocation, update, release and other operations. Downlink network devices obtain, update, rebind and release prefixes by using the four-/two-message exchange mechanism similar to that for allocating addresses. However, prefix allocation is different from address allocation in the following aspects:

- In message exchange using the prefix delegation, the Confirm and Decline messages are not used.
- If a DHCPv6 client moves to a new link and needs to check whether the prefix information is available, it performs confirmation through Rebind and Reply message exchange.
- The IA type in various messages is IA_PD.

For the message exchange using the prefix delegation, refer to the section "Requesting/Allocating Addresses".

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable the DHCPv6 server function for the interface.

The DHCPv6 server function is effective only on a layer-3 interface.

Prefix Delegation of the DHCPv6 Server

- By default, the DHCPv6 server has no configuration pool and is not configured with prefixes.
- You can run the **ipv6 dhcp pool** command to create a configuration pool.
- You can run the **prefix-delegation** command to allocate specified prefixes to a specific DHCPv6 client.
- You can run the **prefix-delegation pool** command to configure a prefix pool so that all prefixes requested by the DHCPv6 client are allocated from this pool.

Enabling the DHCPv6 Client Prefix Request Function on an Interface

By default, an interface is not enabled with the DHCPv6 client prefix request function.

You can run the **ipv6 dhcp client pd** command to enable or disable the DHCPv6 client prefix request function for the interface.

The DHCPv6 client prefix request function is effective only on a layer-3 interface.

5.3.3 Stateless Service

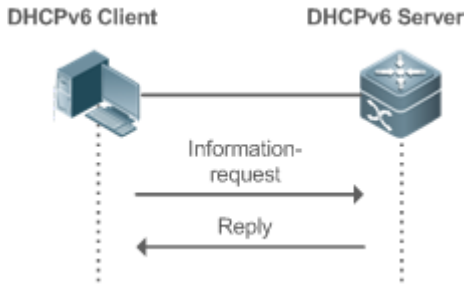
When a DHCPv6 client needs only configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters which cannot be obtained through a stateless automatic address configuration protocol, such as the DNS server address.

Working Principle

Network hosts serve as DHCPv6 clients to exchange messages with the DHCPv6 server to obtain and update configuration parameters.

Message Exchange Using the Stateless Service

Figure 5-12



- A DHCPv6 client sends an Information-request message to a DHCPv6 server to request stateless messages. Usually, this message does not contain the DUID of the specified DHCPv6 server.
- The DHCPv6 server sends a Reply message containing the configuration parameters to the DHCPv6 client.

Related Configuration

Enabling the DHCPv6 Server Function on an Interface

- By default, an interface is not enabled with the DHCPv6 server function.
- You can run the **ipv6 dhcp server** command to enable or disable the DHCPv6 server function for the interface.

⚠ The DHCPv6 server function is effective only on a layer-3 interface.

Stateless Service of a DHCPv6 Server

- By default, the DHCPv6 server has no configuration pool and is not configured with configuration parameters.
- You can run the **ipv6 dhcp pool** command to create a configuration pool.
- You can run the **dns-server** command to add a DNS server.
- You can run the **domain-name** command to add a domain name.
- You can run the **option52** command to add the IPv6 address of the CAPWAP AC.

Stateless Service of a DHCPv6 Client

- By default, an interface is not enabled with the stateless service of the DHCPv6 client.

- If a host receives an RA message containing the O flag, it will enable the stateless service.

5.3.4 Relay Service

When the DHCPv6 client and DHCPv6 server are on different links, the DHCPv6 client can relay related messages to the DHCPv6 server through the DHCPv6 relay agent. The DHCPv6 server also relays the response to the DHCPv6 client through the relay agent.

Working Principle

When receiving a message from the DHCPv6 client, the DHCPv6 relay agent creates a Relay-forward message. This message contains the original message from the DHCPv6 client and some options added by the relay agent. Then, the relay agent sends the Relay-forward message to a specified DHCPv6 server or a specified multicast address FF05::1:3.

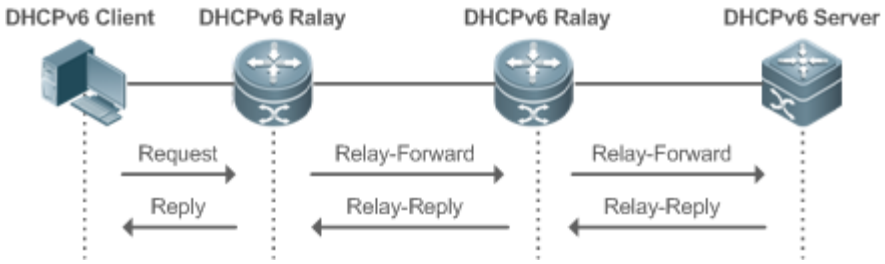
After receiving the Relay-forward message, the DHCPv6 server extracts the original message from the DHCPv6 client f for processing. Then, the DHCPv6 server constructs a response to the original message, encapsulates the response in a Relay-reply message, and then sends the Relay-reply message to the DHCPv6 relay agent.

After receiving the Relay-reply message, the DHCPv6 relay agent extracts the original message from the DHCPv6 server for processing, and forwards the message to the DHCPv6 client.

Multi-level relay agents are allowed between the DHCPv6 client and DHCPv6 server.

DHCPv6 Relay Agent

Figure 5-13



- The DHCPv6 relay agent performs message encapsulation and decapsulation between the DHCPv6 client and DHCPv6 server to enable communication between the DHCPv6 client and DHCPv6 server on different links.

5.3.5 Address Notifying

The DHCPv6 server obtains IPv6 addresses and MAC address of the terminals and notifies them to the authentication module for auditing.

Working Principle

In a subnet without a DHCPv6 Relay device, if IANA address allocating and address notifying are enabled on the DHCPv6 server, the server gets the source MAC addresses from packets and recognizes them as the MAC addresses of terminals. After allocating or renewing IPv6 addresses to the terminals, the IPv6 server notifies to the authentication module the

terminals' MAC and IPv6 addresses, which the module syncs to the authentication server together with IPv4 information. And based on all the received information, the authentication server authenticates or records the treminals.

Related Configuration

Adderess Notifying

- By default, address notifying is disabled.
- Run the **ipv6 dhcp notify** command to enabled address notifying.

5.4 Configuration

Configuration	Description and Command	
Configuring the DHCPv6 Server	(Mandatory) It is used to create a configuration pool.	
	ipv6 dhcp pool	Configures a configuration pool for a DHCPv6 server.
	(Optional) It is used to allocate addresses.	
	iana-address prefix	Configures the address prefixes to be allocated on the DHCPv6 server.
	(Optional) It is used to allocate prefixes.	
	prefix-delegation	Configures prefixes of statically bound addresses on the DHCPv6 server.
	prefix-delegation pool	Configures the DHCPv6 server to allocate prefixes from a local prefix pool.
	ipv6 local pool	Configures a local IPv6 prefix pool.
	(Optional) It is used to allocate configuration parameters.	
	dns-server	Configures the DNS server on the DHCPv6 server.
	domain-name	Configures the domain name of the DHCPv6 server.
	option52	Configures the IPv6 address of the CAPWAP AC on the DHCPv6 server.
	(Mandatory) It is used to enable the DHCPv6 server service.	
	ipv6 dhcp server	Enables the DHCPv6 server service on an interface.
Configuring the DHCPv6 Relay	(Mandatory) It is used to enable the DHCPv6 relay agent service.	
	ipv6 dhcp relay destination	Configures the DHCPv6 relay agent function.

Configuration	Description and Command	
Configuring the DHCPv6 Client	⚠ (Mandatory) It is used to request addresses or prefixes.	
	ipv6 dhcp client ia	Enables the DHCPv6 client and requests IANA addresses.
	ipv6 dhcp client pd	Enables the DHCPv6 client and requests address prefixes.
	⚠ (Optional) It is used to enable a host that receives an RA message to request stateless service through the DHCPv6 client.	
	ipv6 nd other-config-flag	Sets the O flag in the RA message on the device that sends the RA message so that the host that receives the RA message can request stateless service through the DHCPv6 client.

5.4.1 Configuring the DHCPv6 Server

Configuration Effect

- An uplink device can automatically allocate DHCPv6 addresses, prefixes and configuration parameters to a downlink device.

Notes

- To provide the DHCPv6 server service, you must specify a DHCPv6 server configuration pool.
- The name of the configuration pool cannot be too long.
- When enabling the DHCPv6 server service, you must specify a configuration pool.
- Only the Switch Virtual Interface (SVI), routed port and L3 aggregate port (AP) support this configuration.

Configuration Steps

↘ Configuring a DHCPv6 Server Configuration Pool

- Mandatory.
- Unless otherwise specified, you should configure a DHCPv6 server configuration pool on all devices that need to provide the DHCPv6 server service.

↘ Configuring the Address Prefixes to Be Allocated on the DHCPv6 Server

- Optional.
- To provide the address allocation service, you should configure address prefixes to be allocated on all devices that need to provide the DHCPv6 server service.

↘ Configuring Prefixes of Static Addresses on the DHCPv6 Server

- Optional.
- To provide the prefix delegation service for statically bound addresses, you should configure prefixes of statically bound addresses on all devices that need to provide the DHCPv6 server service.

Configuring the DHCPv6 Server to Allocate Prefixes from a Local Prefix Pool

- Optional.
- To provide the prefix delegation service, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring a Local IPv6 Prefix Pool

- Optional.
- To provide the prefix delegation service through a prefix pool, you should specify a local prefix pool on all devices that need to provide the DHCPv6 server service.

Configuring the DNS Server on the DHCPv6 Server

- Optional.
- To allocate DNS servers, you should configure the DNS server on all devices that need to provide the DHCPv6 server service.

Configuring Domain Names on the DHCPv6 Server

- Optional.
- To allocate domain names, you should configure domain names on all devices that need to provide the DHCPv6 server service.

Configuring the IPv6 Address of the CAPWAP AC on the DHCPv6 Server

- Optional.
- To allocate CAPWAP AC information, you should configure the IPv6 address of the CAPWAP AC on all devices that need to provide the DHCPv6 server service.

Enabling the DHCPv6 Server Service

- Mandatory.
- Unless otherwise specified, you should enable the DHCPv6 server service on specific interfaces of all devices that need to provide the DHCPv6 server service.

Verification

The DHCPv6 server allocates addresses, prefixes or configuration parameters for the DHCPv6 client.

- The DHCPv6 client obtains the required information.
- The DHCPv6 server successfully creates a local binding.

Related Commands

Configuring a DHCPv6 Server Configuration Pool

Command	**ipv6 dhcp pool** *poolname*
Parameter Description	***poolname***: Indicates the name of a user-defined DHCPv6 configuration pool.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 dhcp pool** command to create a DHCPv6 server configuration pool. After configuring this command, you may enter the DHCPv6 pool configuration mode, in which you can configure the pool parameters such as the prefix and DNS server. After creating a DHCPv6 server configuration pool, you can run the **ipv6 dhcp server** command to associate the configuration pool with the DHCPv6 server service on an interface.

Configuring the IA_NA Address Prefix for the DHCPv6 Server

Command	**iana-address prefix** *ipv6-prefix/prefix-length* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
Parameter Description	*ipv6-prefix/prefix-length*: Indicates an IPv6 address prefix and the prefix length. **lifetime**: Sets the valid time of the address allocated to a client. This keyword must be configured together with *valid-lifetime* and *preferred-lifetime*. *valid-lifetime***:** Indicates the valid time of the address allocated to a client. *preferred-lifetime*: Indicates the time when an address is preferentially allocated to a client.
Command Mode	Interface configuration mode
Usage Guide	Run the **iana-address prefix** command to configure IA_NA address prefixes for a DHCPv6 server, some of which are allocated to the client. When receiving an IA_NA address request from a client, the DHCPv6 server selects an available address according to the IA_NA address range and allocates the address to the client. When the client does not use this address, the DHCPv6 server marks this address as available for another client.

Configuring Prefixes of Statically Bound Addresses on the DHCPv6 Server

Command	**prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [*lifetime*]
Parameter Description	*ipv6-prefix/prefix-length*: Indicates an IPv6 address prefix and the prefix length. *client-DUID*: Indicates the DUID of a client. *lifetime*: Sets the time when the client can use this prefix.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **prefix-delegation** command to manually configure a prefix list for an IA_PD of a client and specify the valid time of these prefixes. Use the *client-DUID* parameter to specify the client to which the address prefix is allocated. The address prefix will be allocated to the first IA_PD of the client. After receiving a request for the address prefix from the client, the DHCPv6 server checks whether a static

	binding is available. If yes, the DHCPv6 server directly returns the static binding. If not, the DHCPv6 server allocates the address prefix from another prefix source.

Configuring the DCHPv6 Server to Allocate Prefixes from a local prefix pool

Command	**prefix-delegation pool** *poolname* [**lifetime** { *valid-lifetime* | *preferred-lifetime* }]
Parameter Description	***poolname*:** Indicates the name of a user-defined local prefix pool. **lifetime:** Sets the valid time of the prefix allocated to a client. This keyword must be configured together with *valid-lifetime* and *preferred-lifetime*. *valid-lifetime*: Indicates the valid time of the prefix allocated to the client. *preferred-lifetime*: Indicates the time when a prefix is preferentially allocated to a client.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	Run the **prefix-delegation pool** command to configure a prefix pool for a DHCPv6 server to allocate prefixes to clients. The **ipv6 local pool** command is used to configure a prefix pool. When receiving a prefix request from a client, the DHCPv6 server selects an available prefix from the prefix pool and allocates the prefix to the client. When the client does not use this prefix, the DHCPv6 server retrieves the prefix .

Configuring a Local IPv6 Prefix Pool

Command	**ipv6 local pool** *poolname prefix/prefix-length assigned-length*
Parameter Description	*poolname*: Indicates the name of a local prefix pool. *prefix/prefix-length***:** Indicates the prefix and prefix length. *assigned-length***:** Indicates the length of the prefix allocated to a user.
Command Mode	Global configuration mode
Usage Guide	Run the **ipv6 local pool** command to create a local prefix pool. If the DHCPv6 server needs prefix delegation, you can run the **prefix-delegation pool** command to specify a local prefix pool. Afterwards, prefixes will be allocated from the specified local prefix pool.

Configuring the DNS Server on the DHCPv6 Server

Command	**dns-server** *ipv6-address*
Parameter Description	*ipv6-address*: Indicates the IPv6 address of the DNS server.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **dns-server** command for multiple times to configure multiple DNS server addresses. A new DNS server address will not overwrite old DNS server addresses.

Configuring Domain Names on the DHCPv6 Server

Command	**domain-name** *domain*
Parameter	*domain*: Defines a domain name to be allocated to a user.

Description	
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **domain-name** command for multiple times to create multiple domain names. A new domain name will not overwrite old domain names.

Configuring the option52 on the DHCPv6 Server

Command	**option52** *ipv6-address*
Parameter Description	*ipv6-address*: Specifies the IPv6 address of the CAPWAP AC.
Command Mode	DHCPv6 pool configuration mode
Usage Guide	You can run the **option52** command to configure IPv6 addresses for the multiple CAPWAP ACs. A new CAPWAP AC IPv6 address will not overwrite old IPv6 addresses.

Enabling the DHCPv6 Server Service

Command	**ipv6 dhcp server** *poolname* **[rapid-commit] [preference** *value***]**
Parameter Description	*poolname*: Indicates the name of a user-defined DHCPv6 configuration pool. **rapid-commit:** Permits the two-message exchange process. **preference** *value***:** Configures the priority of the advertise message, ranging from 0 to 255. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	Run the **ipv6 dhcp server** command to enable the DHCPv6 service on an interface. When the **rapid-commit** keyword is configured, the two-message exchange with a client is permitted during allocation of address prefixes and other configurations. After this keyword is configured, if the Solicit message from a client contains the **rapid-commit** option, the DHCPv6 server will send a Reply message directly. If **preference** is set to a non-0 value, the advertise message sent by the DHCPv6 server contains the **preference** option. The **preference** field affects the server selection by a client. If an advertise message does not contain this field, the value of **preference** is considered **0**. If the value of **preference** received by the client is 255, the client sends a request to the server immediately to obtain configurations. The DHCPv6 client, server, and relay functions are mutually exclusive. An interface can be configured with only one function at a time.

Configuration Example

Configuring the DHCPv6 Server

Configuration Steps	● Configure a configuration pool named "pool1". ● Configure the IA_NA address prefix for the DHCPv6 server. ● Configure prefixes of statically bound addresses on the DHCPv6 server.

	• Configure two DNS servers. • Configure the domain name. • Enable the DHCPv6 server service on an interface.
	Ruijie# configure terminal Ruijie(config)# ipv6 dhcp pool pool1 Ruijie(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000 Ruijie(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac Ruijie(config-dhcp)# dns-server 2008:1::1 Ruijie(config-dhcp)# dns-server 2008:1::2 Ruijie(config-dhcp)# domain-name example.com Ruijie(config-dhcp)#exit Ruijie(config)# interface GigabitEthernet 0/1 Ruijie(config-if)# ipv6 dhcp server pool1
Verification	• Run the **show ipv6 dhcp pool** command to display the created configuration pool.
	Ruijie# show ipv6 dhcp pool DHCPv6 pool: pool1 Static bindings: Binding for client 0003000100d0f82233ac IA PD prefix: 2008:2::/64 preferred lifetime 3600, valid lifetime 3600 IANA address range: 2008:50::1/64 -> 2008:50::ffff:ffff:ffff:ffff/64 preferred lifetime 1000, valid lifetime 2000 DNS server: 2008:1::1 DNS server: 2008:1::2 Domain name: example.com

Common Errors

- The specified pool name is too long.
- The number of the configuration pools exceeds the system limit (256).
- The configuration is performed on other interfaces than the Switch Virtual Interface (SVI), routed port and L3 AP port.
- The number of interfaces configured with the DHCPv6 server service exceeds the system limit (256).
- The specified value of **valid lifetime** is smaller than that of **preferred lifetime**.

- An invalid IA_NA address is specified.
- The number of address ranges exceeds the system limit (20).
- When prefixes of statically bound addresses are configured, the specified DUIDs are too long.
- The number of prefixes of statically bound addresses exceeds the system limit (1024).
- When a local prefix pool is configured, the specified value of **valid lifetime** is smaller than that of **preferred lifetime**.
- The number of DNS servers exceeds the system limit (10).
- The number of domain names exceeds the system limit (10).
- The number of option52 addresses exceeds the system limit (10).

5.4.2 Configuring the DHCPv6 Relay

Configuration Effect

- A DHCPv6 relay agent can be configured for address allocation, prefix delegation and parameter allocation to enable communication between the DHCPv6 client and server on different links.

Notes

- A destination address must be specified. If the destination address is a multicast address (such as FF05::1:3), you also need to specify an egress interface.

Configuration Steps

↘ Configuring the DHCPv6 Relay Agent Function

- Mandatory.
- Unless otherwise specified, you should configure the DHCPv6 relay agent function on all devices that need to provide the DHCPv6 relay agent service.

Verification

- The DHCPv6 client and DHCPv6 server exchange messages through the relay agent.
- Check whether the interface is enabled with the DHCPv6 relay.
- Check whether the DHCPv6 relay agent can receive and send messages.

Related Commands

↘ Configuring the DHCPv6 Relay Agent Function

Command	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]
Parameter Description	*ipv6-address*: Specifies the destination address of the relay agent. *interface-type*: Specifies the type of the destination interface (optional). *interface-number*: Specifies the destination interface number (optional).
Command	Interface configuration mode

Mode	
Usage Guide	All DHCPv6 packets from clients received by an interface enabled with the DHCPv6 relay function will be encapsulated and sent to a specified destination address (or multiple destination addresses) through a specified interface (optional).

Configuration Example

Configuring the DHCPv6 Relay

Configuration Steps	Specify an interface enabled with the relay service to forward received DHCPv6 client packets to a specified destination address through the specified interface (optional).
	`Ruijie#configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#interface vlan 1` `Ruijie(config-if)#ipv6 dhcp relay destination 3001::2` `Ruijie(config-if)#ipv6 dhcp relay destination ff02::1:2 vlan 2`
Verification	Run the **show ipv6 dhcp relay destination all** command to display the configured destination addresses.
	`Interface:VLAN 1` `Destination address(es)  Output Interface` `3001::2` `ff02::1:2  VLAN 2`

Common Errors

- The configuration is performed on other interfaces than the Switch Virtual Interface (SVI), routed port and L3 AP port.

5.4.3 Configuring the DHCPv6 Client

Configuration Effect

- Enable a device to automatically request IPv6 addresses or related parameters from a server.

Notes

- The configuration must be performed on layer-3 interfaces.

Configuration Steps

Enabling the DHCPv6 Client and Requesting IANA Addresses

- Mandatory.

- Unless otherwise specified, you should enable the DHCPv6 client address request function on all devices that need to request addresses.

Enabling the DHCPv6 Client and Requesting Address Prefixes

- Mandatory.
- Unless otherwise specified, you should enable the DHCPv6 client prefix request function on all devices that need to request prefixes.

Enabling the Stateless Service of the DHCPv6 Client

- It is mandatory if the DHCPv6 client needs to obtain configuration parameters.

Verification

- Check whether the interface is enabled with the DHCPv6 client and check the addresses, prefixes and other configuration obtained on the interface.

Related Commands

Enabling the DHCPv6 Address Request Function

Command	**ipv6 dhcp client ia** [**rapid-commit**]
Parameter Description	**rapid-commit:** Permits the simplified message exchange process.
Command Mode	Interface configuration mode
Usage Guide	If the DHCPv6 client mode is not enabled, this command will enable the DHCPv6 client mode on the interface. After the **ipv6 dhcp client ia** command is configured, an IANA address request will be sent to the DHCPv6 server. The **rapid-commit** keyword permits the two-message exchange process between the client and server. If this keyword is configured, the Solicit message sent by the client contains the **rapid-commit** option.

Enabling the DHCPv6 Client Prefix Request

Command	**ipv6 dhcp client pd** *prefix-name* [**rapid-commit**]
Parameter Description	*prefix-name*: Indicates a IPv6 general prefix. **rapid-commit:** Permits the simplified message exchange process.
Command Mode	Interface configuration mode
Usage Guide	If the DHCPv6 client mode is not enabled, this command will enable the DHCPv6 client mode on the interface. After the **ipv6 dhcp client pd** command is configured, a prefix request will be sent to the DHCPv6 server. After receiving the prefix, the client will save the prefix in the IPv6 general prefix pool. Then, other commands and applications can use this prefix.

	The **rapid-commit** keyword permits the two-message exchange process between the client and server. If this keyword is configured, the Solicit message sent by the client contains the **rapid-commit** option.

Configuring Stateless Service

Command	**ipv6 nd other-config-flag**
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	Configure this command on a host that sends the RA message. Then, the host that receives the RA message obtains stateless configurations through the DHCPv6 client.

Configuration Example

Enabling the DHCPv6 Address Request Function

Configuration Steps	● Configure the DHCPv6 client address request function on an interface.
	`Ruijie(config)# interface GigabitEthernet 0/1` `Ruijie(config-if)# ipv6 dhcp client ia`
Verification	● Run the **show ipv6 dhcp interface** command to display whether the interface is enabled with the DHCPv6 client.
	`Ruijie#show ipv6 dhcp interface GigabitEthernet 0/1` `GigabitEthernet 0/1 is in client mode` `  Rapid-Commit: disable`

Enabling the DHCPv6 Client Prefix Request

Configuration Steps	● Configure the DHCPv6 client prefix request function on an interface.
	`Ruijie(config)# interface GigabitEthernet 0/1` `Ruijie(config-if)# ipv6 dhcp client pd pd_name`
Verification	● Run the **show ipv6 dhcp interface** command to display whether the interface is enabled with the DHCPv6 client.
	`Ruijie#show ipv6 dhcp interface GigabitEthernet 0/1` `GigabitEthernet 0/1 is in client mode` `  Rapid-Commit: disable`

Enabling the DHCPv6 Stateless Service

Configuration Steps	● Configure this command on an interface that sends the RA message.
	Ruijie# configure terminal Ruijie(config)# interface GigabitEthernet 0/1 Ruijie(config-if)# ipv6 nd other-config-flag
Verification	● Run the **show ipv6 dhcp interface** command to display whether an interface of the host obtains configuration parameters.
	Ruijie#show ipv6 dhcp interface GigabitEthernet 0/2 GigabitEthernet 0/2 is in client mode DNS server: 2001::1 Rapid-Commit: disable

Common Errors

- The DHCPv6 client address request is enabled on non-layer-3 interfaces.
- The DHCPv6 address request is enabled on interfaces enabled with the DHCPv6 relay or DHCPV6 server.
- The DHCPv6 client prefix request is enabled on non-layer-3 interfaces.
- The DHCPv6 prefix request is enabled on interfaces enabled with the DHCPv6 relay or DHCPV6 server.

5.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears DHCPv6 bindings.	**clear ipv6 dhcp binding** [*ipv6-address*]
Clears DHCPv6 server statistics.	**clear ipv6 dhcp server statistics**
Clears conflicted addresses on the DHCPv6 server.	**clear ipv6 dhcp conflict** { *ipv6-address* | * }
Clears the statistics on sent and received packets after the DHCPv6 relay is enabled on the current device.	**clear ipv6 dhcp relay statistics**
Restarts the DHCPv6 client.	**clear ipv6 dhcp client** *interface-type interface-number*

Displaying

Description	Command
Displays the DUID of a device.	**show ipv6 dhcp**
Displays address bindings on the DHCPv6 server.	**show ipv6 dhcp binding** [*ipv6-address*]
Displays DHCPv6 interface.	**show ipv6 dhcp interface** [*interface-name*]
Displays DHCPv6 pool.	**show ipv6 dhcp pool** [*poolname*]
Displays conflicted DHCPv6 addresses.	**show ipv6 dhcp conflict**
Displays the statistics on the DHCPv6 server.	**show ipv6 dhcp server statistics**
Displays the destination address of the DHCPv6 relay agent.	**show ipv6 dhcp relay destination** { **all** | *interface-type interface-number* }
Displays the statistics on sent and received packets after the DHCPv6 relay is enabled on a device.	**show ipv6 dhcp relay statistics**
Displays the local IPv6 prefix pool.	**show ipv6 local pool** [*poolname*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs DHCPv6.	**debug ipv6 dhcp** [**detail**]

6 Configuring DNS

6.1 Overview

A Domain Name System (DNS) is a distributed database containing mappings between domain names and IP addresses on the Internet, which facilitate users to access the Internet without remembering IP strings that can be directly accessed by computers. The process of obtaining an IP address through the corresponding host name is called domain name resolution (or host name resolution).

Protocols and Standards

- RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

6.2 Applications

Application	Description
Static Domain Name Resolution	Performs domain name resolution directly based on the mapping between a domain name and an IP address on a device.
Dynamic Domain Name Resolution	Obtains the IP address mapped to a domain name dynamically from a DNS server on the network.

6.2.1 Static Domain Name Resolution

Scenario

- Preset the mapping between a domain name and an IP address on a device.
- When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Deployment

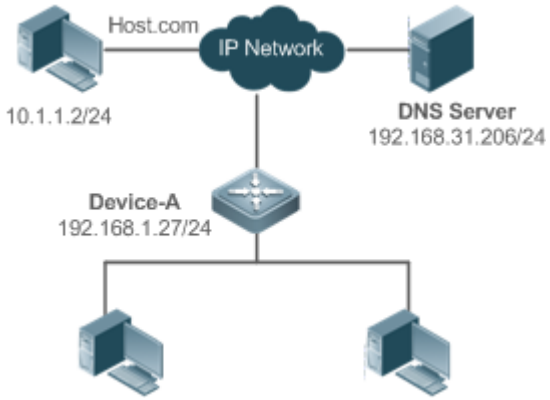
- Preset the mapping between a domain name and an IP address on a device.

6.2.2 Dynamic Domain Name Resolution

Scenario

- DNS Server is deployed on the network to provide the domain name service.
- Domain name "host.com" is deployed on the network.
- Device-A applies to DNS Server for domain name "host.com".

Figure 6-1 Dynamic Domain Name Resolution



Deployment

- Deploy DNS Server as the DNS server of Device-A.

6.3 Features

Basic Concepts

DNS

The DNS consists of a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on the network, and implements mutual conversion between the domain names and IP addresses. Both the TCP and UDP port IDs of DNS are 53, and generally a UDP port is used.

Features

Feature	Description
Domain Name Resolution	IP addresses are obtained based on domain names from a DNS server or a local database.

6.3.1 Domain Name Resolution

Working Principle

Static Domain Name Resolution

Static domain name resolution means that a user presets the mapping between a domain name and an IP address on a device. When you perform domain name operations (such as Ping and Telnet) through application programs, the system can resolve the IP address without being connected to a server on the network.

Dynamic Domain Name Resolution

Dynamic domain name resolution means that when a user perform domain name operations through application programs, the DNS resolver of the system queries an external DNS server for the IP address mapped to the domain name.

The procedure of dynamic domain name resolution is as follows:

13. A user application program (such as Ping or Telnet) requests the IP address mapped to a domain name from the DNS resolver of the system.
14. The DNS resolver queries the dynamic cache at first. If the domain name on the dynamic cache does not expire, the DNS resolver returns the domain name to the application program.
15. If all domain names expire, the DNS resolver initiates a request for domain name-IP address conversion to the external DNS server.
16. After receiving a response from the DNS server, the DNS resolver caches and transfers the response to the application program.

Related Configuration

Enabling Domain Name Resolution

- By default, domain name resolution is enabled.
- Run the **ip domain-lookup** command to enable domain name resolution.

Configuring the IP Address Mapped to a Static Domain Name

- By default, no mapping between a domain name and an IP address is configured.
- Run the **ip host** command to specify the IPv4 address mapped to a domain name.
- Run the **ipv6 host** command to specify the IPv6 address mapped to a domain name.

Configuring a DNS Server

- By default, no DNS server is configured.
- Run the **ip name-server** command to configure a DNS server.

6.4 Configuration

Configuration	Description and Command	
Configuring Static Domain Name Resolution	⚠ Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip host	Configures the IPv4 address mapped to a domain name.
	ipv6 host	Configures the IPv6 address mapped to a domain name.
Configuring Dynamic Domain Name Resolution	⚠ Optional.	
	ip domain-lookup	Enables domain name resolution.
	ip name-server	Configures a DNS server.

6.4.1 Configuring Static Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name on a local device.

Configuration Steps

Enabling Domain Name Resolution

- The domain name resolution function is enabled by default.
- If this function is disabled, static domain name resolution does not take effect.

Configuring the IP Address Mapped to a Domain Name

- (Mandatory) Domain names to be used must be configured with mapped IP addresses.

Verification

- Run the **show run** command to check the configuration.
- Run the **show hosts** command to check the mapping between the domain name and the IP address.

Related Commands

Configuring the IPv4 Address Mapped to a Domain Name

Command	**ip host** *host-name ip-address*
Parameter Description	*host-name*: indicates a domain name. *ip-address*: indicates a mapped IPv4 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the IPv6 Address Mapped to a Domain Name

Command	**ipv6 host** *host-name ipv6-address*
Parameter Description	*host-name*: indicates a domain name. *ipv6-address*: indicates a mapped IPv6 address.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Static Domain Name Resolution

Configuration Steps	● Set the IP address of static domain name www.test.com to 192.168.1.1 on a device. ● Set the IP address of static domain name www.testv6.com to 2001::1 on a device.

	Ruijie#configure terminal Ruijie(config)# ip host www.test.com 192.168.1.1 Ruijie(config)# ipv6 host www.testv6.com 2001::1 Ruijie(config)# exit
Verification	Run the **show hosts** command to check whether the static domain name entry is configured.
	Ruijie#show hosts Name servers are: Host type Address TTL(sec) www.test.com static 192.168.1.1 --- www.testv6.com static 2001::1 ---

6.4.2 Configuring Dynamic Domain Name Resolution

Configuration Effect

The system resolver resolves the IP address mapped to a domain name through a DNS server.

Configuration Steps

↘ Enabling Domain Name Resolution

- Domain name resolution is enabled by default.
- If this function is disabled, dynamic domain name resolution does not take effect.

↘ Configuring a DNS Server

- (Mandatory) To use dynamic domain name resolution, you must configure an external DNS server.

Verification

- Run the **show run** command to check the configuration.

Related Commands

↘ Configuring a DNS Server

Command	**ip name-server**{ *ip-address* | *ipv6-address* }
Parameter Description	*ip-address*: indicates the IPv4 address of the DNS server. *Ipv6-address*: indicates the IPv6 address of the DNS server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Dynamic Domain Name Resolution

Scenario **Figure 6-2**	
	Device resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	Set the IP address of the DNS server to 192.168.10.1 on the device.
	DEVICE#configure terminal DEVICE(config)# ip name-server 192.168.10.1 DEVICE(config)# exit
Verification	Run the **show hosts** command to check whether the DNS server is specified.
	Ruijie(config)#show hosts Name servers are: 192.168.10.1 static Host type Address TTL(sec)

6.5 Monitoring

Clearing

⚠ Running the **clear** command during device operation may cause data loss or even interrupt services.

Description	Command
Clears the dynamic host name cache table.	**clear host** [*host-name*]

Displaying

Description	Command
Displays DNS parameters.	**show hosts** [*host-name*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the DNS function.	**debug ip dns**

7 Configuring FTP Server

7.1 Overview

The File Transfer Protocol (FTP) server function enables a device to serve as an FTP server. In this way, a user can connect an FTP client to the FTP server and upload files to and download files from the FTP server through FTP.

A user can use the FTP server function to easily obtain files such as syslog files from a device and copy files to the file system of the device through FTP.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)
- RFC3659: Extensions to FTP
- RFC2228: FTP Security Extensions
- RFC2428: FTP Extensions for IPv6 and NATs
- RFC1635: How to Use Anonymous FTP

7.2 Applications

Application	Description
Providing FTP Services in a LAN	Provides the uploading and downloading services for a user in a Local Area Network (LAN).

7.2.1 Providing FTP Services in a LAN

Scenario

Provide the uploading and downloading services for a user in a LAN.

As shown in Figure 7-1, enable the FTP server function only in a LAN.

- G and S are enabled with the FTP server function and layer-2 transparent transmission function respectively.
- A user initiates a request for FTP uploading and downloading services.

Figure 7-1

Remarks	G is an egress gateway device. S is an access device.

Deployment

- G is enabled with the FTP server function.
- As a layer-2 switch, S provides the function of layer-2 transparent transmission.

7.3 Features

Basic Concepts

FTP

FTP is a standard protocol defined by the IETF Network Working Group. It implements file transfer based on the Transmission Control Protocol (TCP). FTP enables a user to transfer files between two networked computers and is the most important approach to transferring files on the Internet. A user can obtain abundant Internet for free through anonymous FTP. In addition, FTP provides functions such as login, directory query, file operation, and other session control. Among the TCP/IP protocol family, FTP is an application-layer protocol and uses TCP ports 20 and 21 for transmission. Port 20 is used to transmit data and port 21 is used to transmit control messages. Basic operations of FTP are described in RFC959.

User Authorization

To connect an FTP client to an FTP server, you should have an account authorized by the FTP server. That is, a user can enjoy services provided by the FTP server after logging in to the FTP server with a user name and password. A maximum of 10 accounts can be configured, a maximum of 2 connections are allowed for each account, and a maximum of 10 connections are supported by the server.

FTP File Transmission Modes

FTP provides two file transmission modes:

- Text transmission mode (ASCII mode): It is used to transfer text files (such as .txt, .bat, and .cfg files). This mode is different from the binary mode in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to local CRC characters, for example, \n in Unix, \r\n in Windows, and \r in Mac. Assume that a file being copied contains ASCII text. If a remote computer does not run Unix, FTP automatically converts the file format to suit the remote computer.
- Binary transmission mode: It is used to transfer program files (for example, .app, .bin and .btm files), including executable files, compressed files and image files without processing data. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

FTP Working Modes

FTP provides two working modes:

Figure 7-2

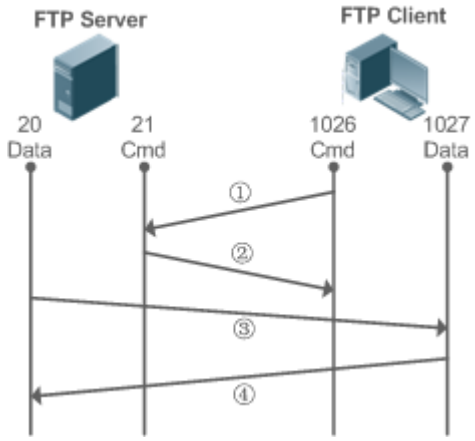
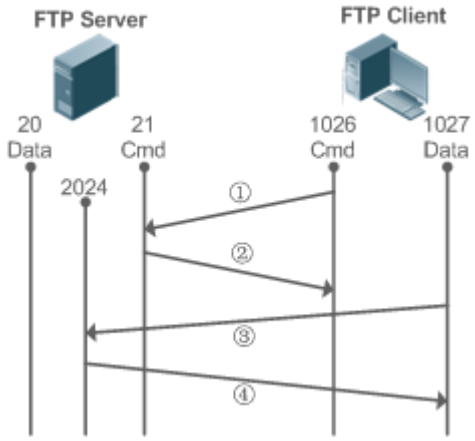


Figure 7-3



- Figure 7-2 shows the active (PORT) mode. The FTP client uses port 1026 to connect to the FTP server through port 21. The client sends commands through this channel. Before receiving data, the client sends the **PORT** command on this channel. The **PORT** command contains information on the channel port (1027) of the client for receiving data. The server uses port 20 to connect to the client through port 1027 for establishing a data channel to receive and transmit data. The FTP server must establish a new connection with the client for data transmission.
- Figure 7-3 shows the passive (PASV) mode. The process for establishing a control channel is similar to that in the PORT mode. However, after the connection is established, the client sends the **PASV** command rather than the **PORT** command. After receiving the **PASV** command, the FTP server enables a high-end port (2024) at random and notifies the client that data will be transmitted on this port. The client uses port 1027 to connect the FTP server through port 2024. Then, the client and server can transmit and receive data on this channel. In this case, the FTP server does not need to establish a new connection with the client.

Supported FTP Commands

After receiving an FTP connection request, the FTP server requires the client to provide the user name and password for authentication.

If the client passes the authentication, the FTP client commands can be executed for operations. The available FTP client commands are listed as follows:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye		mget		rename	system
cd	get	mkdir	passive		type
cdup		mls	put	rmdir	user
close	ls		pwd		

For usage of these FTP client commands, please refer to your FTP client software document. In addition, many FTP client tools (such as CuteFTP and FlashFXP) provide the graphic user interface. These tools facilitate operations by freeing users from configuring FTP commands.

Overview

Feature	Description
Enabling the FTP Server Function	Provides the functions of uploading, downloading, displaying, creating and deleting files for an FTP client.

7.3.1 Enabling the FTP Server Function

Working Principle

The basic working principle is described in the previous chapter. Ruijie devices provide FTP services after the user name, password, and top-level directory are configured.

Related Configuration

↘ Enabling the FTP Server Function Globally

The FTP server function is disabled by default.

Run the **ftp-server enable** command to enable the FTP server function.

You must enable the FTP server function globally before using it.

↘ Configuring a User Name, Password, and Top-Level Directory

There is no authorized user or top-level directory by default.

Run the **ftp-server username password** and **ftp-server topdir** commands to set an authorized user and top-level directory.

The three configurations above are mandatory; otherwise, the FTP server function cannot be enabled.

7.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to enable an FTP server.	
	ftp-server enable	Enables the FTP server function.
	ftp-server login timeout	Configures Login timeout for an FTP session.
	ftp-server login times	Configures the valid login count.
	ftp-server topdir	Configures the top-level directory of the FTP server.
	ftp-server username password	Configures a user name and password.
	Optional.	
	ftp-server timeout	Configures the idle timeout of an FTP session.

7.4.1 Configuring Basic Functions

Configuration Effect

- Create an FTP server to provide FTP services for an FTP client.

Notes

- The user name, password, and top-level directory need to be configured.
- To enable the server to close an abnormal session within a limited period, you need to configure the idle timeout of a session.

Configuration Steps

Enabling the FTP Server Function

- Mandatory.
- Unless otherwise noted, enable the FTP server function on every router.

Configuring a Top-Level Directory

- Mandatory.
- Unless otherwise noted, configure the top-level directory as the root directory on every router.

Configuring a User Name and Password for Login

- Mandatory.
- The lengths of the user name and password are restricted.

Configuring the Login Timeout for an FTP Session

- Optional.
- When the client is disconnected from the server due to an error or other abnormal causes, the FTP server may not know that the user is disconnected and continues to keep the connection. Consequently, the FTP connection is occupied for a long time and the server cannot respond to the login requests of other users. This configuration can ensure that other users can connect to the FTP server within a period of time upon an error.

Verification

Connect an FTP client to the FTP server.

- Check whether the client is connected.
- Check whether operations on the client are normal.

Related Commands

Enabling the FTP Server Function

Command	**ftp-server enable**
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	The client cannot access the FTP server unless the top-level directory, user name and password are configured. Therefore, it is recommended that you configure the top-level directory, user name and password for login by referring to the subsequent chapters before enabling the service for the first time.

Configuring the Valid Login Count

Command	**ftp-server login times***times*
Parameter Description	*times:* Indicates the valid login count, ranging from 1 to 10.
Command Mode	Global configuration mode
Usage Guide	The valid login count refers to the number of times you can perform account verification during an FTP session. The default value is 3, which means that your session will be terminated if you enter an incorrect user name or password for three times and other users can go online.

Configuring the Login Timeout for an FTP Session

Command	**ftp-server login timeout***timeout*

Parameter Description	*timeout*: Indicates the login timeout, ranging from 1 to 30 minutes.
Command Mode	Global configuration mode
Usage Guide	The login timeout refers to the maximum duration that the session lasts since being established. If you do not pass the password verification again during the login timeout, the session will be terminated to ensure that other users can log in.

Configuring the Top-Level Directory of the FTP Server

Command	**ftp-servertopdir***directory*
Parameter Description	*directory:* Indicates the user access path.
Command Mode	Global configuration mode
Usage Guide	If the top-level directory of the server is set to "/syslog", the FTP client can access only the files and directories in the "/syslog" directory on the device after login. Due to restriction on the top-level directory, the client cannot return to the upper directory of "/syslog".

Configuring a User Name and Password for Server Login

Command	**ftp-server username** *username* **password** [*type*] *password*
Parameter Description	*username*: Indicates a user name. *type*: 0 or 7. 0 indicates that the password is not encrypted (plaintext) and 7 indicates that the password is encrypted (cipher text). *password*: Indicates a password.
Command Mode	Global configuration mode
Usage Guide	The FTP server does not support anonymous login; therefore, a user name must be configured. A user name consists of up to 64 characters including letters, half-width digits and symbols without spaces. A password consists of only letters or digits. Spaces at the beginning and end of the password are ignored. Spaces inside the password are viewed as part of the password. A plaintext password consists of 1 to 25 characters. A cipher text password consists of 4 to 52 characters. User names and passwords must match. A maximum of 10 users can be configured. A username is exclusively associated with a password. Up to ten users can be configured.

Configuring the Idle Timeout for an FTP Session

Command	**ftp-Server timeout** *time*
Parameter Description	*time*: Indicates the idle timeout, ranging from 1 to 3,600 minutes.
Command	Global configuration mode

Mode	
Usage Guide	The idle timeout of a session refers to the duration from the end of an FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command operation (for example, after a file is completely transferred), the server starts to count the idle time again, and stops when the next FTP client command operation arrives. Therefore, the configuration of the idle timeout has no effect on some time-consuming file transfer operations.

Displaying Server Status

Command	**show ftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display FTP server status.

Debugging

Command	**debug ftp-server pro/err**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to debug message/error events of the FTP server.

Configuration Example

Creating an FTP Server on an IPv4 Network

Scenario	● A TCP connection is established for transmission from a server to a client.
Configuration Steps	● Enable the FTP server function. ● Configure the top-level directory/syslog. ● Set the user name **user** and password to **password**. ● Set the session idle timeout to 5 minutes.
	`Ruijie(config)#ftp-server username user` `Ruijie(config)#ftp-server password password` `Ruijie(config)#ftp-server timeout 5` `Ruijie(config)#ftp-server topdir /` `Ruijie(config)#ftp-server enable`
Verification	● Run the **show ftp-server** command to check whether the configuration takes effect.
	`Ruijie#show ftp-server`

```
    ftp-server information
==================================
enable : Y
topdir : tmp:/
timeout: 10min
username:aaaa         password:(PLAINT)bbbb         connect num[2]
    [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]
                               client IP:192.168.21.26[3927]
    [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
                               client IP:192.168.21.26[3929]
username:a1           password:(PLAINT)bbbb         connect num[0]
username:a2           password:(PLAINT)bbbb         connect num[0]
username:a3           password:(PLAINT)bbbb         connect num[0]
username:a4           password:(PLAINT)bbbb         connect num[0]
username:a5           password:(PLAINT)bbbb         connect num[0]
username:a6           password:(PLAINT)bbbb         connect num[0]
username:a7           password:(PLAINT)bbbb         connect num[0]
username:a8           password:(PLAINT)bbbb         connect num[0]
username:a9           password:(PLAINT)bbbb         connect num[0]
```

Common Errors

- No user name is configured.
- No password is configured.
- No top-level directory is configured.

7.5 Monitoring

Displaying

Description	Command
Displays the FTP server configuration.	show ftp-server

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the FTP server error events.	**debug ftp-server err**
Debugs the FTP server message events.	**debug ftp-server pro**

8 Configuring FTP Client

8.1 Overview

The File Transfer Protocol (FTP) is an application of TCP/IP. By establishing a connection-oriented and reliable TCP connection between the FTP client and server, a user can access a remote computer that runs the FTP server program.

An FTP client enables file transfer between a device and the FTP server over the FTP protocol. A user uses the client to send a command to the server. The server responds to the command and sends the execution result to the client. By means of command interaction, the user can view files in the server directory, copy files from a remote computer to a local computer, or transfer local files to a remote computer.

FTP is intended to facilitate sharing of program/data files and encourage remote operation (by using programs). Users do not need to be concerned with differences of different files systems on different hosts. Data is transmitted in an efficient and reliable manner. FTP enables remote file operation securely.

Ruijie FTP clients are different from standard FTP clients that run interactive commands. Instead, you enter the **copy** command in CLI to perform control-connection instructions such as **open**, **user**, and **pass**. After a control connection is established, the file transfer process starts, and then a data connection is established to upload or download files.

Old devices support TFTP. However, TFTP is used to transfer small files whereas FTP is used to transfer large files. Implementing FTP on a device enables the file transfer between the local device and other clients or servers.

Protocols and Standards

- RFC959: FILE TRANSFER PROTOCOL (FTP)

8.2 Applications

Application	Description
Uploading a Local File to a Remote Server	Local and remote files need to be shared, for example, uploading a local file to a remote server.
Downloading a File from a Remote Server to a Local Device	Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

8.2.1 Uploading a Local File to a Remote Server

Scenario

Local and remote files need to be shared, for example, uploading a local file to a remote server.

As shown in Figure 8-1, resources are shared only on the Intranet.

Figure 8-1

Deployment

- Implement only communication on the Intranet.
- Enable file uploading on the FTP client.
- Enable file uploading on the FTP server.

8.2.2 Downloading a File from a Remote Server to a Local Device

Scenario

Local and remote files need to be shared, for example, downloading a file from a remote server to a local device.

As shown in Figure 8-2, resources are shared only on the Intranet.

Figure 8-2

Deployment

- Implement only communication on the Intranet.
- Enable file downloading on the FTP client.
- Enable file downloading on the FTP server.

8.3 Features

Basic Concepts

Uploading FTP Files

Upload files from an FTP client to an FTP server.

Downloading FTP Files

Download files from an FTP server to an FTP client.

FTP Connection Mode

An FTP client and an FTP server can be connected in the active or passive mode.

FTP Transmission Mode

The transmission between an FTP client and an FTP server is available in two modes, namely, text (ASCII) and binary (Binary).

Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server.

Overview

Feature	Description
Uploading FTP Files	Uploads files from an FTP client to an FTP server.
Downloading FTP Files	Downloads files from an FTP server to an FTP client.
FTP Connection Mode	Specifies the connection mode between an FTP client and an FTP server.
FTP Transmission Mode	Specifies the transmission mode between an FTP client and an FTP server.
Specifying the Source Interface IP Address for FTP Transmission	Configures a source IP address of an FTP client for communication with an FTP server.

8.3.1 Uploading FTP Files

FTP enables file uploading. Start the FTP client and FTP server simultaneously, and upload files from the FTP client to the FTP server.

8.3.2 Downloading FTP Files

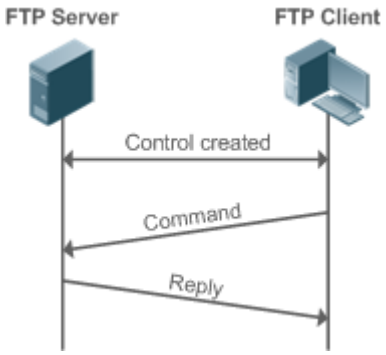
FTP enables file downloading. Start the FTP client and FTP server simultaneously, and download files from the FTP server to the FTP client.

8.3.3 FTP Connection Mode

FTP needs to use two TCP connections: one is a control link (command link) that is used to transfer commands between the FTP client and server; the other one is a data link that is used to upload or download data.

1. Control connection: Some simple sessions are enabled with the control connection only. A client sends a command to a server. After receiving the command, the server sends a response. The process is shown in Figure 8-3.

Figure 8-3 Control Connection



2. Control connection and data connection: When a client sends a command for uploading or downloading data, both the control connection and data connection need to be established.

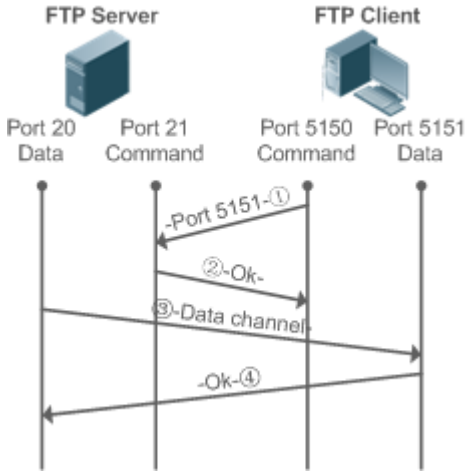
FTP supports two data connection modes: active (PORT) and passive (PASC). The two modes are different in establishing a data connection.

- Active mode

In this mode, an FTP server connects to an FTP client actively when a data connection is established. This mode comprises four steps:

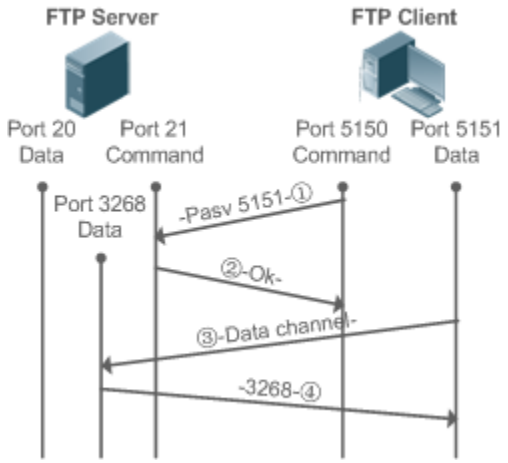
1. The client uses source port 5150 to communicate with the server through port 21 as shown in Figure 8-4 to send a connection request and tell the server that the port to be used is port 5151.
2. After receiving the request, the server sends a response OK(ACK). The client and server exchanges control signaling by console ports.
3. The server enables port 20 as the source port to send data to port 5151 of the client.
4. The client sends a response. Data transmission ends.

Figure 8-4 Active (PORT) Mode



- Passive mode

- Figure 8-5 Passive (PASV) Mode
  -



This mode is often set by the **passive** command. When a data connection is established, the FTP server is connected to the FPT client passively. This mode comprises four steps:

1. In the passive mode, the client initializes the control signaling connection. The client uses source port 5150 to connect to the server through port 21 as shown in Figure 8-5, and runs the **passive** command to request the server to enter the PASV mode.
2. The server agrees to enter the PASV mode, selects a port number greater than 1024 at random, and tells the port number to the client.
3. After receiving the message, the client uses port 5151 as shown in Figure 8-5 to communicate with the server through port 3268. Here, port 5151 is the source port and port 3268 is the destination port.
4. After receiving the message, the server sends data and responds an ACK(OK) response.

After the data connection is established, you can perform file uploading and downloading. Besides, you can perform some operations on the server file from the client.

The control connection for command and feedback transmission is always present whereas the data connection is established as required. Only an FTP client has the right to select and set the PASV or PORT mode. The FTP client sends a command to establish a data connection. Ruijie FTP clients use the PASV mode by default.

8.3.4 FTP Transmission Mode

FTP provides two transmission modes: text (ASCII) and binary (Binary). At present, Ruijie FTP clients support both the ASCII and Binary modes and use the BINARY mode by default.

- ASCII mode

The difference between the ASCII and Binary modes lies in carriage return and line feed processing. In ASCII mode, carriage return and line feed are changed to a local Carriage Return Character (CRC), for example, \n in Unix, \r\n in Windows, and \r in Mac.

- Binary mode

The Binary mode can be used to transfer executable files, compressed files and image files without processing data. For example, a text file needs to be transferred from Unix to Windows. When the Binary mode is used, the line breaks in Unix will not be converted from \r to \r\n; therefore in Windows, this file has no line feeds and displays many black squares. Therefore, Binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

8.3.5 Specifying the Source Interface IP Address for FTP Transmission

An FTP client is configured with a source IP address for communication with an FTP server. In this way, the FTP client connects to the server and shares files with the server through the specified source IP address.

8.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to configure the functions of an FTP client.	
	copy flash	Uploads a file.
	copy ftp	Downloads a file.
Configuring Optional Functions	(Optional) It is used to configure the working mode of the FTP client.	
	ftp-client port	Sets the connection mode to active (port).
	ftp-client ascii	Sets the transmission mode to ASCII.
	ftp-client source-address	Configures the source IP address of the FTP client.
	default ftp-client	Restores the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.

8.4.1 Configuring Basic Functions

Configuration Effect

- Implement file uploading and downloading.

Notes

- Pay attention to the command formats for uploading and downloading.

Configuration Steps

↘ Uploading a File

- This configuration is mandatory when a file needs to be uploaded.

- Configure the FTP URL as the destination address of **copy** in Privileged EXEC mode.

Downloading a File

- This configuration is mandatory when a file needs to be downloaded.
- Configure the FTP URL as the source address of **copy** in Privileged EXEC mode.

Verification

- Check whether the uploaded file exists on the FTP server.
- Check whether the downloaded file exists at the destination address.

Related Commands

Uploading a File

Command	**copy flash:**[*local-directory/*]*local-file* **ftp:** *//username:password@dest-address*[*/remote-directory*]*/remote-file*
Parameter Description	*local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Specifies a local file to be uploaded. *username*: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory. *dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server. *remote-file:* Renames the file on the server. ⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to upload a file from the flash of a local device to an FTP server.

Downloading an FTP File

Command	**copy ftp:***//username:password@dest-address*[*/remote-directory*]*/remote-file* **flash:**[*local-directory/*]*local-file*
Parameter Description	*username*: Specifies a user name for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server, consisting of no more than 32 bytes and excluding delimiters such as /, :, @ and space. This parameter is mandatory. *dest-address:* Specifies an IP address for the FTP server. *remote-directory:* Specifies a directory on the server.

	remote-file: Specifies a file to be downloaded. *local-directory:* Specifies a directory on the local device. If it is not specified, it indicates the current directory. *local-file:* Renames the file in the local flash. ⚠ The directory specified by the *local-directory* field must have been created on the device. This command will not automatically create a directory.
Command Mode	Global configuration mode
Usage Guide	Run this command to download a file from an FTP server to the flash of a local device.

Configuration Example

Uploading a File

Configuration Steps	Upload the **local-file** file in the **home** directory of a device to the **root** directory of an FTP server whose user name is **user**, password is **pass** and IP address is **192.168.23.69** and name the file as **remote-file**.
	`Ruijie# copy flash: home/local-file ftp://user:pass@192.168.23.69/root/remote-file`
Verification	Check whether the **remote-file** file exists on the FTP server.

Downloading a File

Configuration Steps	Download the **remote-file** file from the **root** directory of an FTP server whose user name is **user**, password is **pass** and IP address is **192.168.23.69** to the **home** directory of a device and save the file as **local-file**.
	`Ruijie# copy ftp://user:pass@192.168.23.69/root/remote-file flash: home/local-file`
Verification	Check whether the **remote-file** file exists in the **home** directory of the flash.

Common Errors

- The command formats for uploading and downloading are incorrect.
- The user name or password is incorrect.

8.4.2 Configuring Optional Functions

Configuration Effect

- Set the connection and transmission modes and configure a source IP address of the client for file uploading and download.

Notes

- N/A

Configuration Steps

Setting the Connection Mode to Active (Port)

- Optional.
- Configure the connection mode of FTP.

Setting the Transmission Mode to ASCII

- Optional.
- Configure the transmission mode of FTP.

Configuring the Source IP Address of the FTP Client

- Optional.
- Configure the source IP address of the FTP client.

Restoring the Default Settings

- Optional.
- Restore the default settings of the FTP client.

Verification

Run the **show run** command to check whether the configuration takes effect.

Related Commands

Setting the Connection Mode to Active (Port)

Command	**ftp-client port**
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Run this command to set the connection mode to active (port). The default connection mode is passive (PASV).

Configuring the Source IP Address of the FTP Client

Command	**ftp-client source-address** {*ip-address* | *ipv6-address* }
Parameter Description	*ip-address:* Specifies the IPv4 address of a local interface. *ipv6-address:* Specifies the IPv6 address of a local interface.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an interface IP address of the client for connection to the server. By default, the client is not configured with a local IP address. Instead, the route selects an IP address for the client.

Setting the Transmission Mode to ASCII

Command	ftp-client ascii
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Run this command to set the transmission mode to ASCII. The default transmission mode is Binary.

Restoring the Default Settings

Command	default ftp-client
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Run this command to restore the default settings, namely, connection mode set to passive (PASV), transmission mode to Binary and source IP address removed.

Configuration Example

Configuring Optional Functions

Configuration Steps	• Set the connection mode of FTP to port. • Set the transmission mode to ASCII. • Set the source IP address to 192.168.23.167.
	Ruijie# configure terminal Ruijie(config)# ftp-client ascii Ruijie(config)# ftp-client port Ruijie(config)# ftp-client source-address 192.168.23.167 Ruijie(config)# end
Verification	Run the **show run** command on the device to check whether the configuration takes effect. Ruijie# show run ! ftp-client ascii ftp-client port ftp-client vrf 123 port ftp-client vrf 123 ascii

	ftp-client source-address 192.168.23.167 !

Common Errors

- The source IP address is not a local IP address.

8.5 Monitoring

Displaying

Description	Command
Displays the FTP client configuration.	**show run**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the FTP Client.	**debug ftp-client**

-

9 Configuring Tunnel Interfaces

9.1 Overview

Tunnel interfaces are virtual interfaces used to implement tunneling. A tunnel interface provides a standard transmission link and you do not need to specify a transport protocol or payload protocol. Each tunnel interface represents a transmission link.

Tunneling function includes the following parts:

- Payload protocol: Is used to encapsulate the data transmitted in tunnels. For example, the IPv4 and IPv6 protocols work as payload protocols. Generic routing encapsulation (GRE) tunnels can carry IPv4 or IPv6 data.
- Bearer protocol: Is used for secondary encapsulation and identification of the data to be transmitted. Among the tunnels described in this document, only the GRE tunnel uses a bearer protocol, that is, the GRE protocol. The other tunnels use the IPv4 and IPv6 protocols. Packets are encapsulated with outer IPv4 and IPv6 headers.
- Transport protocol: Is used to transmit the data encapsulated for the second time through a bearer protocol. Ruijie products use the widely applied IPv4 and IPv6 protocols as transport protocols.

The tunnel mode can be used to set up communication between two private networks running the same protocol through a heterogeneous public network.

Tunneling is applicable to the following scenarios:

- Because tunneling supports different payload protocols, it allows the communication between local networks running non-IP protocols through a single network (IP network). Because tunneling operates on routes running transport protocols (IP protocols), it allows wider application of the protocols with hop limit.
- Tunneling allows discrete subnets to be connected through a single network (IP network).
- Tunneling allows the virtual private network (VPN) feature to be enabled on wide area networks (WANs).

Encapsulated data is transmitted through tunnels, which is a complex process. In some cases, you need to pay attention to the following changes:

- Because a tunnel is a logical link, it appears to be a single hop in routing. However, actually its path cost may be more than one hop. When you use a tunnel for transmission, note that the route of the tunnel link is different from the actual route.
- When you configure a firewall or an access control list (ACL), take the tunnel configuration into consideration. The transmission bandwidth and maximum transmission unit (MTU) allowed by payload protocols are smaller than the theoretical values.

Protocols and Standards

- RFC2784: Generic Routing Encapsulation (GRE)
- RFC2890: Key and Sequence Number Extensions to GRE

- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC3068: An Anycast Prefix for 6to4 Relay Routers
- RFC3964: Security Considerations for 6to4
- RFC4023: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- RFC4087: IP Tunnel MIB
- RFC4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC4797: Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC5158: 6to4 Reverse DNS Delegation Specification
- RFC5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC5332: MPLS Multicast Encapsulations
- RFC5579: Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC5969: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
- RFC6245: Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC6343: Advisory Guidelines for 6to4 Deployment
- RFC6372: 6to4 Provider Managed Tunnels
- RFC6654: Gateway-Initiated IPv6 Rapid Deployment on IPv4 Infrastructures (GI 6rd)
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-cai-softwire-6rd-mib-03 Definitions of Managed Objects for 6rd
- draft-howard-isp-ip6rdns-05 Reverse DNS in IPv6 for Internet Service Providers
- draft-tsou-softwire-6rd-multicast-02 IPv6 Multicast Using Native IPv4 Capabilities in a 6rd Deployment
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

9.2 Applications

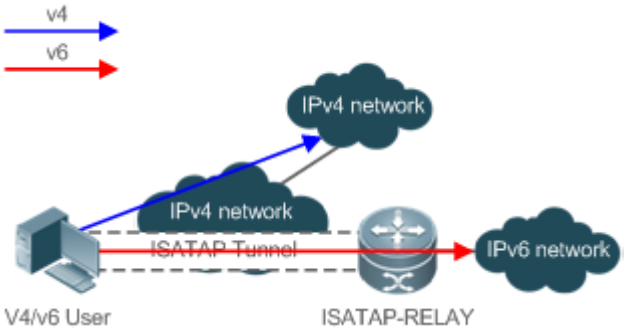
Application	Description
Accessing the IPv6 Sites on a Campus Network	Accesses the IPv6 sites on a campus network.

9.2.1 Accessing the IPv6 Sites on a Campus Network

Scenario

IPv6 servers are deployed on some campus networks, and PCs need to access the servers. The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) can be used to realize the access.

Figure 9-1



Remarks	ISATAP-RELAY supports tunneling. Users on the campus network can access IPv4 servers directly through the IPv4 network, but need to access IPv6 servers through the ISATAP tunnel.

Deployment

- IPv4 and IPv6 users access the IPv4 network by using IPv4 addresses.
- IPv4 and IPv6 users access the IPv6 network through the ISATAP tunnel.
- The ISATAP tunnel is established between PCs and the ISATAP-RELAY router.

9.3 Features

Basic Concepts

Tunnel MTU

- The MTU of a tunnel interface is smaller than that of a regular interface, such as a regular IPv4 over IPv4 tunnel. The maximum amount of data carried by a packet transmitted over the Ethernet is 1,460 bytes, not including the two IP headers. Therefore, the MTU of a tunnel interface is 1,480 bytes, not 1,500 bytes of a standard Ethernet interface.

Tunnel Path MTU

- A tunnel interface represents a virtual link. For an IPv4 over IPv4 tunnel, the MTU of the tunnel interface is the MTU of the tunnel link, that is, the MTU of the path between the local and peer ends of the tunnel When the routing path between the local and peer ends is changed, the MTU of the path may also be changed, which will affect the MTU of the tunnel interface.

Tunnel Encapsulation Limit

- Tunnel encapsulation is supported. For example, an IPv4 packet can be encapsulated with two or more IPv4 headers and then transmitted in an IPv4 over IPv4 tunnel. Tunnel encapsulation is intended for security protection and used sparingly. The amount of data to be transmitted is reduced after tunnel encapsulation. After routing through the forwarding information base (FIB), if the outbound interface is another tunnel interface, tunnel encapsulation occurs. If

the outbound interface is the local tunnel interface, infinite encapsulation occurs. (Ruijie products can detect this case and give prompts.)

Overview

Feature	Description
Tunnel Reachability Detection	Checks whether tunnel links are available.
Tunnel MTU Auto-Adjustment	Dynamically adjusts the MTU of a tunnel interface based on the changes of the path MTU of the tunnel link.
Tunnel Encapsulation Limit	Increases the maximum number of nested encapsulations of a packet based on actual requirements. (This feature is rarely used.)
Tunnel Data Validity Check	Adds checksum to the data transmitted in GRE tunnels to check whether an error occurs during transmission.

9.3.1 Tunnel Reachability Detection

Tunnel reachability detection is used to check whether the virtual link of a tunnel is available. Before this feature is enabled, a tunnel is considered as available if routing through the FIB based on the destination IP address is successful. After this feature is enabled, the criteria for determining tunnel availability are more accurate.

Working Principle

Each side of a tunnel periodically sends a keepalive packet to the other side. If one side does not receive a keepalive packet in the specified time, the tunnel is considered unavailable. Tunnel reachability detection is deployed only on one side of the tunnel.

Construction of a keepalive packet (Take IPv4 over IPv4 as an example): The packet is encapsulated with three IPv4 headers. The source address of the outer IPv4 header is the local address of the tunnel, and the destination address is the peer address. The local address and destination address of the middle IPv4 header are contrary to those of the outer and inner IPv4 headers.

One end of the tunnel encapsulates a keepalive packet with the preceding three IPv4 headers and sends it to the peer end. The peer end decapsulates the packet and returns the packet to the local end.

Upon receiving the packet, the local end of the tunnel which initially sends the packet continues to decapsulate the packet until only one IPv4 header remains. If the packet is a keepalive packet, the tunnel link is considered available.

Related Configuration

↘ Enabling Reachability Detection on Tunnel Interfaces

By default, reachability detection is disabled on tunnel interfaces.

To enable or disable reachability detection on tunnel interfaces, run the **keepalive** command.

For tunnel encapsulation, if the outermost tunnel is reachable, the other inner tunnels are also reachable.

9.3.2 Tunnel MTU Auto-Adjustment

The MTU of a tunnel interface is subject to the MTU of the tunnel link, that is, the path MTU. The MTU of the tunnel interface will be changed if a path is changed or the path MTU is changed. The tunnel MTU auto-adjustment feature is used to detect these changes and automatically adjust the MTU of the tunnel interface on the changes.

Working Principle

When a device receives an Internet Control Message Protocol (ICMP) error packet (PACKET TOO BIG), if the packet is encapsulated with a tunneled packet (an encapsulated IP packet), the faulty tunnel can be located based on the encapsulation information. The MTU of the tunnel interface will be changed based on the information in the "PACKET TOO BIG" packet.

Related Configuration

↘ Enabling Tunnel MTU Auto-Adjustment on Tunnel Interfaces

By default, tunnel MTU auto-adjustment is disabled on tunnel interfaces.

To enable or disable tunnel MTU auto-adjustment on tunnel interfaces, run the **tunnel path-mtu-discovery** command.

For tunnel encapsulation, tunnel MTU auto-adjustment needs to be enabled only for the outermost tunnel. The MTU of each inner tunnel is equal to the MTU of the outermost tunnel minus the length of the outer encapsulated header.

9.3.3 Tunnel Encapsulation Limit

In many cases, tunnel encapsulation is a deployment error and is actively deployed only in few cases. By default, Ruijie products allow four nested encapsulations of a packet at most. Administrators can use a command to change the limit.

Working Principle

If the peer end of tunnel interface A is a regular outbound interface, Ruijie products consider Tunnel Interface A as a regular tunnel interface.

If the peer end of tunnel interface A is another tunnel interface, Ruijie products consider Tunnel Interface A as a nested tunnel interface. If the outbound tunnel is a regular tunnel interface, Tunnel Interface A is called a single-nested tunnel. If the outbound tunnel is a single-nested tunnel, Tunnel Interface A is called a double-nested tunnel.

If the peer end of tunnel interface A is itself, infinite recursive encapsulation occurs. When Ruijie products detect infinite recursive encapsulation, they will output logs and disable Tunnel Interface A.

If the peer end of the tunnel is another tunnel interface, routing is performed based on the peer address of the tunnel interface. The actual outbound interface will be determined after multiple times of routing.

If the number of nested encapsulations on a tunnel interface exceeds the upper limit, Ruijie products will output logs and disable the tunnel interface.

Note that the tunnel encapsulation limit is a device-based feature and is different from the maximum number of encapsulated headers in a packet over a network.

Related Configuration

Configuring the Tunnel Encapsulation Limit on Tunnel Interfaces

By default, the maximum number of nested encapsulations of a packet on a tunnel interface is four. To change this limit, run the **tunnel nested-limit** command.

9.3.4 Tunnel Data Validity Check

In a GRE tunnel enabled with data validity check, the receiver checks the validity of the packets sent by the peer end to determine whether the packets are tampered or modified accidentally during transmission. In the case of long distance transmission, if the encapsulated data transmitted in GRE tunnels does not have similar validity check capabilities, you can enable tunnel data validity check.

Working Principle

A GRE tunnel calculates the checksum of the data to be encapsulated at the sender and encapsulates the checksum in the packet before sending the packet out.

Upon receiving the packet, the receiver recalculates the checksum and compares the calculated value to the checksum field in the packet. If the two do not match, the receiver considers that the packet has an error and discards it.

Related Configuration

Enabling Tunnel Data Validity Check on Tunnel Interfaces

By default, data validity check is disabled on tunnel interfaces.

To enable or disable data validity check on tunnel interfaces, run the **tunnel checksum** command.

Tunnel data validity check takes effect only when it is enabled on both ends of a GRE tunnel.

9.4 Configuration

Configuration	Description and Command	
Configuring Tunnel Interfaces	(Mandatory) It is used to create tunnels.	
	Interface tunnel	Creates a tunnel interface.
	tunnel source	Configures the local address of a tunnel.
Configuring a Tunnel Mode	(Optional) It is used to configure a tunnel mode.	
	tunnel mode	Configures a tunnel encapsulation mode.
Configuring a Peer Address	(Optional) It is used to configure the peer address of a tunnel.	
	tunnel destination	Configures the peer address of a tunnel.
Configuring the VPN of a VPN Tunnel	(Optional) It is used to configure the VPN tunnel.	
	tunnel vrf	Configures the VPN tunnel.

Configuration	Description and Command	
Configuring the TOS of a Tunnel	(Optional) It is used to configure the type of service (TOS) of a tunnel.	
	tunnel tos	Configures the TOS of a tunnel.
Configuring the TTL of a Tunnel	(Optional) It is used to configure the time to live (TTL) of a tunnel.	
	tunnel ttl	Configures the TTL of a tunnel.
Configuring the Tunnel Encapsulation Limit	(Optional) It is used to configure the maximum number of nested encapsulations of a packet.	
	tunnel nested-limit	Configures the maximum number of nested encapsulations of a packet.
Configuring Tunnel Data Validity Check	(Optional) It is used to enable data validity check for GRE tunnels.	
	tunnel checksum	Enables data validity check for GRE tunnels.
Configuring a Tunnel Key	(Optional) It is used to configure the check key of a tunnel.	
	tunnel key	Configures the check key of a GRE tunnel.

9.4.1 Configuring Tunnel Interfaces

Configuration Effect

- Create a tunnel interface.

Configuration Steps

Creating a Tunnel Interface

- Run the **interface tunnel** *number* command in global configuration mode to create a tunnel interface.
- The tunneling service is available only after a tunnel interface is created.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel interface is created successfully.

Related Commands

Configuring a Tunnel Interface

Command	**interface tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Checking the Tunnel Configuration

Command	**show interfaces tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Creating a Tunnel Interface

Configuration Steps	● Create a tunnel interface.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# end
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: ..... Tunnel protocol/transport is gre ip

Common Errors

- A tunnel interface cannot be created due to memory deficiency.
- A tunnel interface cannot be created due to insufficient hardware resource deficiency.

9.4.2 Configuring a Tunnel Mode

Configuration Effect

- Configure a tunnel encapsulation mode in tunnel interface configuration mode when you need to use a tunnel in non-default encapsulation mode.

Configuration Steps

Configuring a Tunnel Mode

- Optional.
- The default encapsulation mode for routers and gateway products is tunnel mode gre ip.

- To change the default encapsulation mode, run the **tunnel mode** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel encapsulation mode is configured.

Related Commands

Configuring a Tunnel Mode

Command	**tunnel mode** { **gre ip | ipv6ip [6to4 | isatap]** }
Parameter Description	Each mode corresponds to different encapsulation format of the packets sent out by the tunnel interface. **gre ip** indicates that a packet is encapsulated with a GRE header and an IPv4 header in sequence and then is transmitted over a new IPv4 network. **ipv6ip** indicates that the tunnel interface carries only IPv6 packets and a packet sent out by the tunnel interface is encapsulated with an IPv4 header and then transmitted over a new IPv4 network. The preceding tunnels are manual tunnels, whereas IPv6IP 6RD, 6to4, and ISATAP are automatic tunnels. During packet encapsulation, the destination IPv4 address is mapped from the destination IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	Both ends of a tunnel must be configured with the same encapsulation mode. Otherwise, the tunnel cannot work.

Configuration Example

Configuring the IPv4 over IPv4 Encapsulation Mode

Configuration Steps	● Configure the IPv4 over IPv4 encapsulation mode on a tunnel interface.
	`Ruijie# configure terminal` `Ruijie(config)# interface tunnel 1` `Ruijie(config-if-Tunnel 1)# tunnel mode ipip` `Ruijie(config)# end`
Verification	● Check the configuration of the tunnel interface.
	`Ruijie# show interfaces tunnel 1` `.....` `Tunnel attributes:` `.....` `  Tunnel protocol/transport is ipv6ip`

Common Errors

- A 6to4 tunnel or ISATAP tunnel is configured for a virtual routing and forwarding (VRF) instance that is already configured with a 6to4/ISATAP tunnel.

9.4.3 Configuring a Local Address

Configuration Effect

- Configure the local address of a tunnel.

Notes

- The local address of a tunnel must match the transport protocol used by the tunnel. Otherwise, the tunnel interface will not be up (be disabled).
- When the local address is specified indirectly by configuring another interface, the local address is the primary IPv4 address or the first global public IPv6 address of IPv6.

Configuration Steps

↘ Configuring a Local Address

- Mandatory.
- Run the **tunnel source** command in tunnel interface configuration mode to specify the local address of a tunnel.

Verification

- Run the **show interfaces tunnel** *number* command to display the local address of the tunnel.

Related Commands

↘ Configuring a Local Address

Command	**tunnel source** { *ip-address* | *interface-name interface-number* }
Parameter Description	**ip-address**: Indicates an IPv4 or IPv6 address. *Interface-name interface-number*: Indicates a Layer-3 interface.
Command Mode	Interface configuration mode
Usage Guide	If you specify an IPv4 or IPv6 address directly, you need to configure the address of the device.

Configuration Example

↘ Configuring a Local Address

Configuration Steps	• Configure the local address of a tunnel as 1.1.1.1.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1

	Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel source 1.1.1.1
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is no set .....

9.4.4 Configuring a Peer Address

Configuration Effect

- A manual tunnel can be used (the tunnel interface is up) only after its peer address is configured.

Notes

- Peer addresses cannot be configured for automatic tunnels.

Configuration Steps

↘ Configuring a Peer Address

- The peer addresses must be configured for all tunnels except 6RD, 6to4, and ISATAP tunnels.
- Run the **tunnel destination** command in interface configuration mode to configure the peer address of a tunnel.

Verification

- Run the **show interfaces tunnel** command to check whether the destination address is configured.

Related Commands

↘ Configuring a Peer Address

Command	**tunnel destination** { *ip-address* }
Parameter Description	***ip-address***: Indicates an IPv4 or IPv6 address.
Command	Interface configuration mode

Mode	
Usage Guide	The peer address of a manual tunnel must be configured. The protocol suite type of the configured peer address must be consistent with the transport protocol used by the tunnel. If they are not consistent, the tunnel interface will be disabled (down).

Configuration Example

Configuring a Peer Address

Configuration Steps	● Configure the peer address of a tunnel as 2.2.2.2.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel destination 2.2.2.2
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip .....

Common Errors

- A peer address is configured for an automatic tunnel.
- The peer address configured for a tunnel is the same as that of another tunnel.

9.4.5 Configuring the VPN of a VPN Tunnel

Configuration Effect

- A device may have multiple network interfaces, which may belong to different VPNs. You can specify the VPN where a tunnel link will be created.

Notes

- If the specified VPN does not exist, the tunnel link can still be created, but the tunnel interface will be disabled (down).

Configuration Steps

Configuring the VPN of a VPN Tunnel

- Optional for all tunnels.
- By default, tunnels connected to other devices on the public network are created.
- To create tunnels connected to the devices on a VPN, run the **tunnel vrf** *vrf-name* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the VPN is configured.

Related Commands

Configuring the VPN of a VPN Tunnel

Command	**tunnel vrf** *vrf-name*
Parameter Description	***vrf-name***: Indicates the VPN where the tunnel is located.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring the VPN of a VPN Tunnel

Configuration Steps	● Configure VPN 1.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel vrf VPN1
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class not set, Tunnel TTL 254

	Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is VPN1 .....

Common Errors

- The transport layer protocol is IPv6, but the VPN uses the VRF of the IPv4 protocol suite.
- The VPN uses multi-protocol VRF, but the address family mapped to the tunneling protocol is not enabled.

9.4.6 Configuring the TOS of a Tunnel

Configuration Effect

- Specify the TOS or Traffic Class field in the transport protocol header.

Notes

- If the TOS or Traffic Class field in the transport protocol header is not specified, the TOS or Traffic Class field of the protocol is copied to the header.

Configuration Steps

↘ Configuring the TOS of a Tunnel

- Optional.
- To change the priority of tunnel data on a network, run the **tunnel tos** command in interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the TOS is configured.

Related Commands

↘ Configuring the TOS of a Tunnel

Command	**tunnel tos** *number*
Parameter Description	***number***: Indicates the TOS of a tunnel.
Command Mode	Interface configuration mode
Usage Guide	By default, if the IPv4 protocol is used for the inner bearer and outer encapsulation in a tunnel, the TOS bytes in the inner IPv4 header are copied to the outer IPv4 header. If the IPv6 protocol is used for the inner bearer and outer encapsulation in a tunnel, the Traffic Class 8 bit in the inner IPv6 header is copied to the outer IPv6 header. In other cases, the TOS field in the outer IPv4 header and the Traffic Class field in the IPv6 header are 0.

Configuration Example

Configuring the TOS of a Tunnel

Configuration Steps	● Configure the TOS of a tunnel.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel tos 2
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is VPN1 .....

9.4.7 Configuring the TTL of a Tunnel

Configuration Effect

- Specify the TTL or hop limit of tunnel encapsulation protocol headers.

Configuration Steps

Configuring the TTL of a Tunnel

- Optional.
- By default, the TTL is 254, which is the maximum value.
- To change the tunnel link length limit, run the **tunnel ttl** command.

Verification

- Run the **show interfaces tunnel** command to check whether the TTL is configured.

Related Commands

Configuring the TTL of a Tunnel

Command	**tunnel ttl** *hop-limit*
Parameter Description	*hop-limit*: Indicates the hop limit of a tunnel.
Command Mode	Global configuration mode
Usage Guide	The hop limit specifies the maximum number of routers that a packet can pass through. The default value is 254. This command is used to change the hop quantity limit.

Configuration Example

Configuring the TTL of a Tunnel

Configuration Steps	● Configure the TTL of a tunnel.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel ttl 3
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is VPN1

9.4.8 Configuring Tunnel Reachability Detection

Configuration Effect

- Determine the availability of tunnels more accurately through tunnel reachability detection.

Configuration Steps

Configuring Tunnel Reachability Detection

- Optional for manual tunnels. Automatic tunnels do not support reachability detection.
- To dynamically monitor the availability of tunnel links, configure tunnel reachability detection in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether tunnel reachability detection is configured.

Related Commands

↘ Configuring Tunnel Reachability Detection

Command	**keepalive** [*seconds* [*retries*]]
Parameter Description	***seconds***: Indicates the interval at which keepalive packets are retransmitted, in the unit of seconds. *retries*: Indicates the number of times keepalive packets are retransmitted.
Command Mode	Interface configuration mode
Usage Guide	Manual tunnels support reachability detection, whereas automatic tunnels do not support it. By default, tunnel reachability detection is disabled. A tunnel interface is up if the route to the destination IP address can be found in the routing table of the device. After tunnel reachability detection is enabled, the tunnel interface is up if keepalive packets are sent and received correctly.

Configuration Example

↘ Configuring Tunnel Reachability Detection

Configuration Steps	● Configure tunnel reachability detection.
	`Ruijie# configure terminal` `Ruijie(config)# interface tunnel 1` `Ruijie(config)# tunnel mode ipv6ipRuijie(config)# keepalive 3 5`
Verification	● Check the configuration of the tunnel interface.
	`Ruijie# show interfaces tunnel 1` `Index(dec):11 (hex):b` `...` `Keepalive interval is 3 sec ,retries 5.`

9.4.9 Configuring Tunnel Path MTU Discovery

Configuration Effect

- Configure tunnel path MTU discovery to allow the MTU of a tunnel interface to be adjusted automatically based on the changes of the route MTU. Before this feature is configured, the MTU of the tunnel interface is equal to the MTU of the transport protocol minus the length of the header encapsulated through a transport protocol.

Configuration Steps

↘ Configuring Tunnel Path MTU Discovery

- Optional for manual tunnels. Automatic tunnels do not support tunnel path MTU discovery.
- To dynamically monitor and adjust the MTUs of tunnel links, configure tunnel path MTU discovery in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether tunnel path MTU discovery is configured.

Related Commands

↘ Configuring Tunnel Path MTU Discovery

Command	**tunnel path-mtu-discovery** [**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*]
Parameter Description	*aging-mins*: Indicates the interval at which the MTU of a tunnel interface ages, in the unit of minutes. **infinite** indicates that the MTU never ages. *mtu-bytes*: Indicates the minimum value of the MTU.
Command Mode	Global configuration mode
Usage Guide	Use this command to realize dynamic monitoring and automatic change of the MTUs of tunnel links. You can configure the monitoring frequency and the lower limit of MTU change. Tunnel path MTU discovery has three states: init, learning, and keep. ● init indicates that detection is not initiated. ● learning indicates that dynamic learning is in progress. ● keep indicates that dynamic MTU adjustment is completed and the next round of adjustment is ready. Tunnel path MTU discovery depends on the "ICMP Packet Too Big" error packet returned by a device. If the packet is filtered by an in-between device, the discovery results will be inaccurate.

Configuration Example

↘ Configuring Tunnel Path MTU Discovery

Configuration Steps	● Configure tunnel path MTU discovery.

	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config)# tunnel mode ipv6ip Ruijie(config)# tunnel path-mtu-discovery
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ... Tunnel transport VPN is no set Path MTU Discovery state:init, ager 10 mins, min MTU 92

Common Errors

- Tunnel path MTU discovery is enabled for automatic tunnels.

9.4.10 Configuring the Tunnel Encapsulation Limit

Configuration Effect

- Change the maximum number of nested encapsulations allowed by the outer protocol of a tunnel.

Notes

- In many cases, the tunnel encapsulation limit does not need to be changed.

Configuration Steps

↘ Configuring the Tunnel Encapsulation Limit

- By default, Ruijie products allow a maximum of four nested encapsulations of a packet. This limit can meet requirements in many scenarios.
- To change the limit, run the **tunnel nested-limit** *number* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the tunnel encapsulation limit is configured.

Related Commands

↘ Configuring the Tunnel Encapsulation Limit

Command	**tunnel nested-limit** *number*
Parameter Description	*number*: Indicates the maximum number of nested encapsulations of a packet.

Command Mode	Interface configuration mode
Usage Guide	Ruijie products automatically discover tunnel multi-encapsulation and prevent excessive nested encapsulations. Only manual tunnels support the tunnel encapsulation limit, whereas automatic tunnels do not support it. The tunnel encapsulation limit is a device-based feature and indicates the maximum number of times a packet is encapsulated from its entrance to the device to exit.

Configuration Example

Configuring the Tunnel Encapsulation Limit

Configuration Steps	● Configure the tunnel encapsulation limit.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode ipv6ip Ruijie(config-if-Tunnel 1)# tunnel nested-limit 8
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 8, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is VPN1 .....

Common Errors

- The tunnel encapsulation limit is configured for automatic tunnels.

9.4.11 Configuring Tunnel Data Validity Check

Configuration Effect

- Configure tunnel data validity check to determine whether the data carried by tunnels is changed during transmission. If the data is changed, it is considered as corrupted and will be discarded. If the data carried by a tunnel does not have the validity check feature, you can enable the data validity check feature of the tunnel.

Notes

- Only GRE tunnels support data validity check.

Configuration Steps

Configuring Tunnel Data Validity Check

- Optional.
- If application protocols do not support data validity check, you can enable the data validity check feature of GRE tunnels.
- To enable tunnel data validity check, run the **tunnel checksum** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether tunnel data validity check is enabled.

Related Commands

Configuring Tunnel Data Validity Check

Command	**tunnel checksum**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to enable the data validity check feature of a GRE tunnel if the service data carried in the GRE tunnel does not support validity check. Data validity check must be configured on both ends of a tunnel. The sender adds the checksum to an encapsulated packet. The receiver calculates the checksum of the packet and compares it to the checksum provided by the sender. If they are consistent, the packet is valid. Otherwise, the packet is invalid.

Configuration Example

Configuring Tunnel Data Validity Check

Configuration Steps	• Configure data validity check in a tunnel.
	`Ruijie# configure terminal` `Ruijie(config)# interface tunnel 1` `Ruijie(config-if-Tunnel 1)# tunnel mode gre ip`

	Ruijie(config-if-Tunnel 1)# tunnel checksum
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 ..... Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 8, current nested number is 0 Tunnel protocol/transport gre ip Key disabled, Sequencing disabled Checksumming of packets enabled Tunnel transport VPN is VPN1 .....

Common Errors

- Data validity check is configured for regular tunnels (non-GRE tunnels).

9.4.12 Configuring a Tunnel Key

Configuration Effect

- By configuring the key of a tunnel interface, you can ensure the security of both ends of the tunnel to some extent, and also prevent malicious probe and attacks.

Notes

- Each packet encapsulated in the GRE format contains the configured key, but the attempt to ensure security through the key is inconsiderate.
- Both ends of a tunnel must use the same key settings.

Configuration Steps

↘ Configuring a Tunnel Key

- Optional.
- You can configure different keys to segregate the data carried in a GRE tunnel.
- To configure a tunnel key, run the **tunnel key** *key-value* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the tunnel key is configured.

Related Commands

Configuring a Tunnel Key

Command	**tunnel key** *key-value*
Parameter Description	*key-value*: Indicates the value of a tunnel key.
Command Mode	Interface configuration mode
Usage Guide	The sender encapsulates the key in a packet. The receiver compares the local key to the key in the packet. If they are inconsistent, the packet is discarded.

Configuration Example

Configuring a Tunnel Key

Configuration Steps	● Configure a tunnel key.
	Ruijie# configure terminal Ruijie(config)# interface tunnel 1 Ruijie(config-if-Tunnel 1)# tunnel mode gre ip Ruijie(config-if-Tunnel 1)# tunnel key 10
Verification	● Check the configuration of the tunnel interface.
	Ruijie# show interfaces tunnel 1 …… Tunnel attributes: Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3 Tunnel config nested limit is 8, current nested number is 0 Tunnel protocol/transport gre ip Key 0xa, Sequencing disabled Checksumming of packets enabled Tunnel transport VPN is VPN1 ……

Common Errors

- Tunnel keys are configured for regular tunnels (non-GRE tunnels).

9.5 Monitoring

Displaying

Description	Command
Displays the information about a tunnel interface.	**show interfaces tunnel** *number*

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables tunnel interface debugging.	**debug tunnel**

10 Configuring Network Communication Test Tools

10.1 Overview

Network communication test tools can be used to check the connectivity of a network and helps you analyze and locate network faults. Network communication test tools include Packet Internet Groper (PING) and Traceroute. Ping is used to check the connectivity and delay of a network. A greater delay indicates a slower network speed. Traceroute helps you learn about the topology of physical and logical links and transmission rate. On a network device, you can run the **ping** and **traceroute** commands to use the two tools respectively.

Protocols and Standards

- RFC792: Internet Control Message Protocol
- RFC4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

10.2 Applications

Application	Description
End-to-End Connectivity Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.
Host Route Test	Both the network device and the destination host are connected to the IP network and configured with IP addresses.

10.2.1 End-to-End Connectivity Test

Scenario

As shown in Figure 10-1, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the end-to-end connectivity test aims to check whether IP packets can be transmitted between the two ends. The target host can be the network device itself. In this case, the connectivity test aims to check the network interface and TCP/IP configurations on the device.

Figure 10-1

Deployment

Execute the ping function on the network device.

10.2.2 Host Route Test

Scenario

As shown in Figure 10-2, Network Device A and Target Host B are connected to the IP network.

If both the network device and the target host are connected to the IP network, the host route test aims to check gateways (or routers) that IP packets pass through between the two ends. Generally, the target host is not within the same IP network segment as the network device.

Figure 10-2

Deployment

Execute the traceroute function on the network device.

10.3 Features

Overview

Feature	Description
Ping Test	Test whether the specified IPv4 or IPv6 address is reachable and display the related information.
Traceroute Test	Display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.

10.3.1 Ping Test

Working Principle

The ping tool sends an Internet Control Message Protocol (ICMP) Request message to the destination host to request the for an ICMP Echo Reply message. In this way, the ping tool determines the delay and the connectivity between the two network devices.

Related Configuration

- Run the **ping** command.

10.3.2 Traceroute Test

Working Principle

The traceroute tool uses the Time To Live (TTL) field in the headers of the ICMP and IP messages for the test First, the traceroute tool on the network device sends an ICMP Request message with TTL 1 to the destination host. After receiving

the message, the first router on the path decreases the TTL by 1. As the TTL becomes 0, the router drops the packets and returns an ICMP time exceeded message to the network device. After receiving this message, the traceroute tool learns that this router exists on this path, and then sends an ICMP Request packet with TTL 2 to the destination host to discover the second router. Each time the traceroute tool increases the TTL in the ICMP Request message by 1 to discover one more router. This process is repeated until a data packet reaches the destination host. After the packet reaches the destination host, the host returns an ICMP Echo message instead of an ICMP time exceeded message to the network device. Then, the traceroute tool finishes the test and displays the path from the network device to the destination host.

Related Configuration

- Run the **traceroute** command.

10.4 Configuration

Configuration	Description and Command	
Ping Test	(Optional) It is used to check whether an IPv4 or IPv6 address is reachable.	
	ping	Executes the Ping function.
Traceroute Test	(Optional) It is used to display the gateways that IPv4 or IPv6 packets pass through when transmitted from the source to the destination.	
	traceroute	Executes the traceroute function.

10.4.1 Ping Test

Configuration Effect

After conducting a ping test on a network device, you can learn whether the network device is connected to the destination host and whether packets can be transmitted between the network device and the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To check whether an IPv4 address is reachable, use the **ping IPv4** command.
- To check whether an IPv6 address is reachable, use the **ping IPv6** command.

Verification

Run the **ping** command to display related information on the command line interface (CLI) window.

Related Commands

↘ **Ping IPv4**

Command	**ping** [**oob** | **ip**] [*address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**] [**interval** millisecond] [**out-interface** interface]
Parameter Description	*oob:* Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *address*: Specifies the destination IPv4 address or domain name. **via**: If a device supports multiple MGMT ports, that is, multiple MGMT ports are displayed in the **show interface brief** command output, you are advised to add **via mgmt xxx** to the ping command. *mgmt-name:* Specifies the MGMT port in OOB mode. *length*: Specifies the length of the data packet. The value ranges from 36 to 18, 024. The default length is 100. *times*: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295 *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. By default, the string is "abcd". *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. **df-bit**: Configures the DF bit of the IP address. When the DF bit is set to 1, the packet is not fragmented. By default, the DF bit is 0. **validate**: Configures whether to verify the response packet. **detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. interface: Specifies the interface for sending the data packets. millisecond: Specifies the interval at which the ping packet is sent. The value ranges from 50 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping function. In Privileged EXEC mode, you can execute the extended ping function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping function, you can specify the number, length and timeout of packets to be sent. Like the basic ping function, related statistics will be output. To use the domain name, you must first configure the domain name server (DNS). For details about the configuration, see *Configuring DNS*.

Ping IPv6

Command	**ping** [**oob** | **ipv6**] [*ip-address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** *millisecond*] [**out-interface** *interface*]
Parameter Description	**oob**: Indicates out-of-band management. This parameter must be configured if the MGMT port is specified as the source port. *address*: Specifies the destination IPv6 address or domain name. *length*: Specifies the length of data packet. The value ranges from 16 to 18, 024. The default length is 100.

	times: Specifies the number of probes. The value ranges from 1 to 4, 294, 967, 295. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *data*: Specifies the data in the packet. The data is a string of 1 to 255 bytes. *source*: Specifies the source IPv6 address or source port of the packet. The loopback interface address, for example, ::1, cannot be used as the source address. **Detail**: Configures whether to display the Echo Reply message in detail. By default, only the exclamation mark (!) and dot (.) are displayed. *interface*: Specifies the interface for sending the data packets. *millisecond*: Specifies the interval at which the ping packet is sent. The value ranges from 10 ms to 300,000 ms. The default interval is 100 ms.
Command Mode	In User EXEC mode, you can execute only the basic ping IPv6 function. In Privileged EXEC mode, you can execute the extended ping IPv6 function. In other configuration modes, you can run the **do** command to execute the extended ping function. For details about the configuration, see the description about the **do** command.
Configuration Usage	When the ping IPv6 function is executed, information about the response (if any) will be displayed, and then related statistics will be output. Using the extended ping IPv6 function, you can specify the number, length and timeout of packets to be sent. Like the basic ping IPv6 function, related statistics will be output. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

↘ Executing the Common Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command.
	Common ping command: Ruijie# ping 192.168.21.26 Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: Ruijie#ping 192.168.21.26 detail Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=100 time=4ms TTL=64

	Reply from 192.168.21.26: bytes=100 time=3ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Reply from 192.168.21.26: bytes=100 time=1ms TTL=64 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping Function

Configuration Steps	In Privileged EXEC mode, run the **ping 192.168.21.26** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3 Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > !! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds: < press Ctrl+C to break > Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

	Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64 Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
Verification	Send twenty 1500-byte packets to the specified IP address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

Executing the Common Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::1** command.
	Common ping command: Ruijie# ping ipv6 2001::1 Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms Detailed ping command: Ruijie#ping 2001::1 detail Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds: < press Ctrl+C to break > Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms

	Reply from 2001::1: bytes=100 time=1ms Reply from 2001::1: bytes=100 time=1ms Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
Verification	Send five 100-byte packets to the specified IP address, and the response information will be displayed in the specified time (2s by default). Finally the statistics is output.

Executing the Extended Ping IPv6 Function

Configuration Steps	In Privileged EXEC mode, run the **ping ipv6 2001::5** command. In addition, specify the length, number, and timeout of the packets.
	Common ping command: Ruijie# ping ipv6 2001::5 length 1500 ntimes 100 data ffff source 2001::9 timeout 3 Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds: < press Ctrl+C to break > !!! !!!!! Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms Detailed ping command: Ruijie#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3 Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds: < press Ctrl+C to break > Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms Reply from 2001::5: bytes=1500 time=1ms

	`Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.`
Verification	Send one hundred 1500-byte packets to the specified IPv6 address, and the response information (if any) will be displayed in the specified time (3s by default). Finally the statistics is output.

10.4.2 Traceroute Test

Configuration Effect

After conducting a traceroute test on a network device, you can learn about the routing topology between the network device and the destination host, and the gateways through which packets are sent from the network device to the destination host.

Notes

The network device must be configured with an IP address.

Configuration Steps

- To trace the route an IPv4 packet would follow to the destination host, run the **traceroute IPv4** command.
- To trace the route an IPv6 packet would follow to the destination host, run the **traceroute IPv6** command.

Verification

Run the **traceroute** command to display related information on the CLI window.

Related Commands

↘ Traceroute IPv4

Command	**traceroute** [**ip**] [*adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]
Parameter Description	*address*: Specifies the destination IPv4 address or domain name. *number*: Specifies the number of probes. The value ranges from 1 to 255. *source*: Specifies the source IPv4 address or source port of the packet. The loopback interface address, for example, 127.0.0.1, cannot be used as the source address. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.
Command Mode	In User EXEC mode, you can execute only the basic traceroute function. In privileged EXEC mode, you can execute the extended traceroute function.
Configuration Usage	The **traceroute** command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

↘ Traceroute IPv6

Command	**traceroute** [**ipv6**] [*address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]
Parameter	*address*: Specifies the destination IPv6 address or domain name.

Description	*number*: Specifies the number of probes. The value ranges from 1 to 255. *seconds*: Specifies the timeout. The value ranges from 1s to 10s. *minimum maximum*: Specifies the minimum and maximum TTL values. The value ranges from 1 to 255.
Command Mode	In User EXEC mode, you can execute only the basic traceroute IPv6 function. In privileged EXEC mode, you can execute the extended traceroute IPv6 function.
Configuration Usage	The traceroute IPv6 command is used to test the network connectivity and accurately locate a fault when the fault occurs. To use the domain name, you must first configure the DNS. For details about the configuration, see *Configuring DNS*.

Configuration Example

Executing the Traceroute Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute 61.154.22.36** command.
	Ruijie# traceroute 61.154.22.36 < press Ctrl+C to break > Tracing the route to 61.154.22.36 1 192.168.12.1 0 msec 0 msec 0 msec 2 192.168.9.2 4 msec 4 msec 4 msec 3 192.168.9.1 8 msec 8 msec 4 msec 4 192.168.0.10 4 msec 28 msec 12 msec 5 202.101.143.130 4 msec 16 msec 8 msec 6 202.101.143.154 12 msec 8 msec 24 msec 7 61.154.22.36 12 msec 8 msec 22 msec
	The preceding test result indicates that the network device accesses host 61.154.22.36 by transmitting packets through gateways 2-7. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute 202.108.37.42** command.

	Ruijie# traceroute 202.108.37.42 < press Ctrl+C to break > Tracing the route to 202.108.37.42 1 192.168.12.1 0 msec 0 msec 0 msec 2 192.168.9.2 0 msec 4 msec 4 msec 3 192.168.110.1 16 msec 12 msec 16 msec 4 * * * 5 61.154.8.129 12 msec 28 msec 12 msec 6 61.154.8.17 8 msec 12 msec 16 msec 7 61.154.8.250 12 msec 12 msec 12 msec 8 218.85.157.222 12 msec 12 msec 12 msec 9 218.85.157.130 16 msec 16 msec 16 msec 10 218.85.157.77 16 msec 48 msec 16 msec 11 202.97.40.65 76 msec 24 msec 24 msec 12 202.97.37.65 32 msec 24 msec 24 msec 13 202.97.38.162 52 msec 52 msec 224 msec 14 202.96.12.38 84 msec 52 msec 52 msec 15 202.106.192.226 88 msec 52 msec 52 msec 16 202.106.192.174 52 msec 52 msec 88 msec 17 210.74.176.158 100 msec 52 msec 84 msec 18 202.108.37.42 48 msec 48 msec 52 msec
	The preceding test result indicates that the network device accesses host 202.108.37.42 by transmitting packets through gateways 1–17, and Gateway 4 is faulty.

Executing the Traceroute IPv6 Function on a Properly Connected Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.

	Ruijie# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1-4. In addition, the time required to reach each gateway is displayed.

Executing the Traceroute IPv6 Function on a Faulty Network

Configuration Steps	In Privileged EXEC mode, run the **traceroute ipv6 3004::1** command.
	Ruijie# traceroute ipv6 3004::1 < press Ctrl+C to break > Tracing the route to 3004::1 1 3000::1 0 msec 0 msec 0 msec 2 3001::1 4 msec 4 msec 4 msec 3 3002::1 8 msec 8 msec 4 msec 4 * * * 5 3004::1 4 msec 28 msec 12 msec
	The preceding test result indicates that the network device accesses host 3004::1 by transmitting packets through gateways 1–5, and Gateway 4 is faulty.

11 Configuring TCP

11.1 Overview

The Transmission Control Protocol (TCP) is a transport-layer protocol providing reliable connection-oriented and IP-based services to for the application layer.

Internetwork data flows in 8-bit bytes are sent from the application layer to the TCP layer, and then fragmented into packet segments of a proper length via the TCP. The Maximum Segment Size (MSS) is usually limited by the Maximum Transmission Unit (MTU) of the data link layer. After that, the packets are sent to the IP layer and then to the TCP layer of a receiver through the network.

To prevent packet loss, every byte is identified by a sequence number via the TCP, and this ensures that packets destined for the peer are received in order. Then, the receiver responds with a TCP ACK packet upon receiving a packet. If the sender does not receive ACK packets in a reasonable Round-Trip Time (RTT), the corresponding packets (assumed lost) will be retransmitted.

- TCP uses the checksum function to check data integrity. Besides, MD5-based authentication can be used to verify data.
- Timeout retransmission and piggyback mechanism are adopted to ensure reliability.
- The Sliding Window Protocol is adopted to control flows. As documented in the Protocol, unidentified groups in a window should be retransmitted.

Protocols and Standards

- RFC 793: Transmission Control Protocol
- RFC 1122: Requirements for Internet Hosts -- Communication Layers
- RFC 1191: Path MTU Discovery
- RFC 1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
- RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022: Management Information Base for the Transmission Control Protocol (TCP)

11.2 Applications

Application	Description
Optimizing TCP Performance	To avoid TCP packet fragmentation on a link with a small MTU, Path MTU Discovery (PMTUD) is enabled.
Detecting TCP Connection Exception	TCP checks whether the peer works normally.

11.2.1 Optimizing TCP Performance

Scenario

For example, TCP connection is established between A and D, as shown in the following figure. The MTU of the link between A and B is 1500 bytes, 1300 bytes between B and C, and 1500 bytes between C and D. To optimize TCP transmission performance, packet fragmentation should be avoided between B and C.

Figure 11-1

Remarks:	A, B, C and D are routers.

Deployment

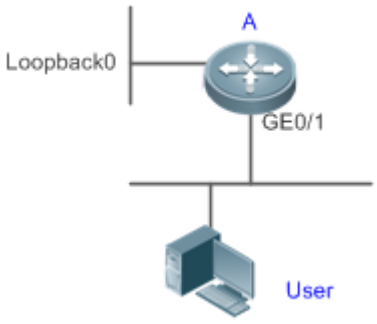
- Enable PMTUD on A and D.

11.2.2 Detecting TCP Connection Exception

Scenario

For example, in the following figure, User logs in to A through telnet but is shut down abnormally, as shown in the following figure. In case of TCP retransmission timeout, the User's TCP connection remains for a long period. Therefore, TCP keepalive can be used to rapidly detect TCP connection exception.

Figure 11-2



Remarks:	A is a router.

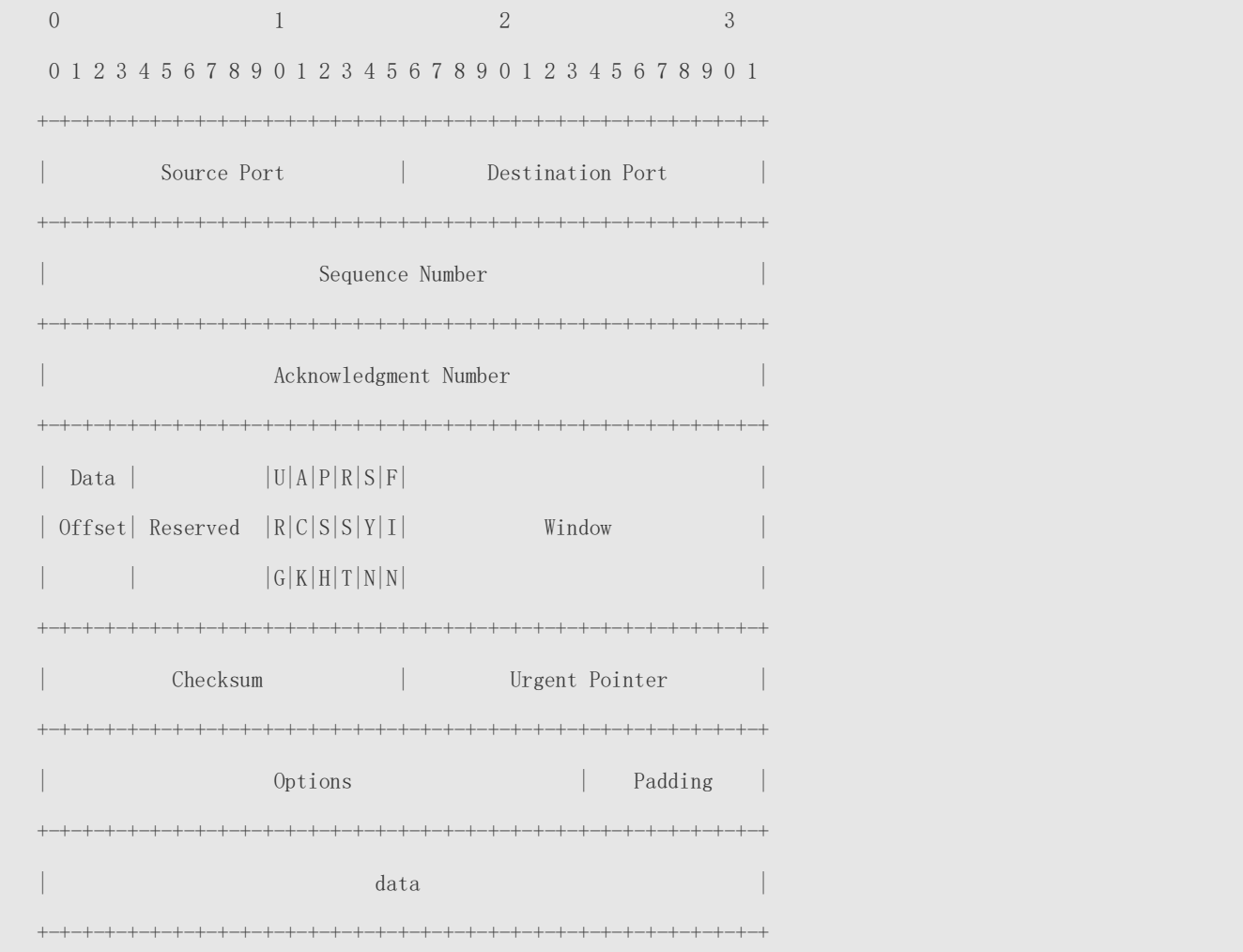
Deployment

- Enable TCP keepalive on A.

11.3 Features

Basic Concepts

TCP Header Format



- **Source Port** is a 16-bit source port number.
- **Destination Port** is a 16-bit destination port number.
- **Sequence Number** is a 32-bit sequence number.
- **Acknowledgment Number** is a 32-bit number that identifies the next sequence number that the receiver is expecting to receive.
- **Data Offset** is a 4-bit number that indicates the total number of bytes in the TCP header (option included) divided by 4.
- A flag bit is 6-bit. URG: the urgent pointer field is significant; ACK: the acknowledgment field is significant; PSH: indicates the push function; RST: resets TCP connection; SYN: synchronizes the sequence number (establishing a TCP connection); FIN: no more data from the sender (closing a TCP connection).

- A 16-bit Window value is used to control flows. It specifies the amount of data that may be transmitted from the peer between ACK packets.
- **Checksum** is a 16-bit checksum.
- **Urgent Pointer** is 16-bit and shows the end of the urgent data so that interrupted data flows can continue. When the URG bit is set, the data is given priority over other data flows.

TCP Three-Way Handshake

- The process of TCP three-way handshake is as follows:

17. A client sends a SYN packet to the server.
18. The server receives the SYN packet and responds with a SYN ACK packet.
19. The client receives the SYN packet from the server and responds with an ACK packet.

- After the three-way handshake, the client and server are connected successfully and ready for data transmission.

Overview

Feature	Description
Configuring SYN Timeout	Configure a timeout waiting for a response packet after an SYN or SYN ACK packet is sent.
Configuring Window Size	Configure a window size.
Configuring Reset Packet Sending	Configure the sending of TCP reset packets after receiving port unreachable messages.
Configuring MSS	Configure an MSS for TCP connection.
Configuring MSS Value for SYN Packet	Modify the MSS value in a SYN packet.
Path MTU Discovery	Discover the smallest MTU on TCP transmission path, and adjust the size of TCP packets based on this MTU to avoid fragmentation.
TCP Keepalive	Check whether the peer works normally.

11.3.1 Configuring SYN Timeout

Working Principle

A TCP connection is established after three-way handshake: The sender sends an SYN packet, the receiver replies with a SYN ACK packet, and then the sender replies with an ACK packet.

- If the receiver does not reply with a SYN ACK packet after the sender sends an SYN packet, the sender keeps retransmitting the SYN packet for certain times or until timeout period expires.
- If the receiver replies with a SYN ACK packet after the sender sends an SYN packet but the sender does not reply with an ACK packet, the receiver keeps retransmitting the SYN ACK packet for certain times or until timeout period expires. (This occurs in the case of SYN flooding.)

Related Configuration

Configuring TCP SYN Timeout

- The default TCP SYN timeout is 20 seconds.
- Run the **ip tcp synwait-time** *seconds* command in global configuration mode to configure an SYN timeout ranging from 5 to 300 seconds.
- In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

The **ip tcp syntime-out** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp synwait-time** command.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.2 Configuring Window Size

Working Principle

Data from the peer is cached in the TCP receiving buffer and subsequently read by applications. The TCP window size indicates the size of free space of the receiving buffer. For wide-bandwidth bulk-data connection, enlarging the window size dramatically promotes TCP transmission performance.

Related Configuration

Configuring Window Size

- Run the **ip tcp window-size** *size* command in global configuration mode to configure a window size ranging from 128 to (65535<< 14) bytes. The default is 65535 bytes. If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.
- The window size advertised to the peer is the smaller value between the configured window size and the free space of the receiving buffer.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.3 Configuring Reset Packet Sending

Working Principle

When TCP packets are distributed to applications, if the TCP connection a packet belongs to cannot be identified, the local end sends a reset packet to the peer to terminate the TCP connection. Attackers may use port unreachable messages to attack the device.

Related Configuration

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Run the **no ip tcp send-reset** command in global configuration mode to disable TCP reset packet sending upon receiving port unreachable messages.

After this function is enabled, attackers may use port unreachable messages to attack the device.

- The **ip tcp not-send-rst** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **no ip tcp send-reset** command.
- In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

11.3.4 Configuring MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment t excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties take the smaller MSS between them as the advertised MSS.

The MSS value is calculated as follows:

- IPv4 TCP: MSS = Outgoing interface MTU –IP header size (20-byte)–TCP header size (20-byte).
- IPv6 TCP: MSS = IPv6 Path MTU –IPv6 header size (40-byte)–TCP header size (20-byte).

- In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.
- The effective MSS is the smaller one between the calculated MSS and the configured MSS.
- If a connection supports certain options, the option length (with **data offset** taken into consideration) should be deducted from an MSS value. For example, 20 bytes for MD5 digest (with **data offset** taken into consideration) should be subtracted from the MSS.

Related Configuration

Configuring MSS

- Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. It ranges from 68 to 1000 bytes. By default, the MSS is calculated based on MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.
- An excessively small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS value by referring to the interface MTU. If the former is bigger, TCP packets will be fragmented and transmission performance will be reduced.

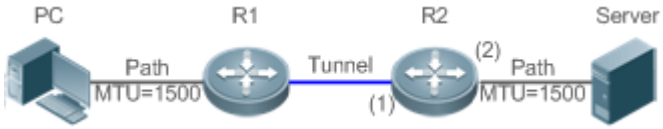
11.3.5 Configuring MSS Value for SYN Packet

Working Principle

When a client initiates a TCP connection, it negotiates with the server on the total amount of data contained in a TCP segment through the MSS field in TCP SYN packets. The MSS value in the SYN packets indicates the largest amount of data that the server sends in a single and unfragmented piece.

For example, in the following figure, the MSS negotiated between a PC and a HTTP server is 1460, but TCP packets carrying 1460-byte data should be fragmented as they cannot directly pass R1 and R2 connected by a tunnel with an MTU of less than 1500. Modify the MSS value in SYN packets on interfaces (1) and (2) of R2 to enable TCP packets to pass R1 and R2.

Figure 11-3



Related Configuration

Configuring MSS Value for TCPv4 SYN Packets

- By default, the MSS value in TCPv4 SYN packets is not modified.
- Run the **ip tcp adjust-mss** *max-segment-size* command in interface configuration mode to set an MSS, which ranges from 500 to 1460 bytes.
- To avoid packet fragmentation in the case of a small path MTU, you may configure an MSS for TCPv4 SYN packets. The MSS in TCPv4 SYN packets will change to the configured value once the device receives the packets. You may configure an MSS value with reference to the interface MTU.

This configuration applies to a new connection but does not take effect for an existing TCP connection.

This function is supported by all products except switches.

Configuring MSS Value for TCPv6 SYN Packets

- By default, the MSS value in TCPv6 SYN packets is not modified.
- Run the **ipv6 tcp adjust-mss** *max-segment-size* command in interface configuration mode to set an MSS for TCPv6 SYN packets, which ranges from 1220 to 1440 bytes.
- To avoid packet fragmentation in the case of a small path MTU, you may configure an MSS for TCPv4 SYN packets. The MSS in TCPv4 SYN packets will change to the configured value once the device receives the packets. You may configure an MSS value with reference to the interface MTU.

This configuration applies to a new TCPv6 connection but does not take effect for an existing TCPv6 connection.

This function is supported by all products except switches.

11.3.6 Path MTU Discovery

Working Principle

The Path MTU Discovery f stipulated in RFC1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 Path MTU Discovery is described as follows:

20. The source sends TCP packets with the Don't Fragment (DF) bit set in the outer IP header.
21. If the outgoing interface MTU value of a router in the TCP path is smaller than the IP packet length, the packet will be discarded and an ICMP error packet carrying this MTU will be sent to the source.
22. Through parsing the ICMP error packet, the source knows the smallest MTU in the path (path MTU) is.
23. The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows: TCP MSS = Path MTU – IP header size – TCP header size.

Related Configuration

Enabling Path MTU Discovery

By default, Path MTU Discovery is disabled.

Run the **ip tcp path-mtu-discovery** command to enable PMTUD in global configuration mode.

In version 10.x, the configuration applies to both IPv4 TCP and IPv6 TCP. In version 11.0 or later, it applies to only IPv4 TCP. TCPv6 PMTUD is enabled permanently and cannot be disabled.

11.3.7 TCP Keepalive

Working Principle

You may enable TCP keepalive to check whether the peer works normally. If a TCP end does not send packets to the other end for a period of time (namely idle period), the latter starts sending keepalive packets successively to the former for several times. If no response packet is received, the TCP connection is considered inactive and then closed.

Related Configuration

Enabling Keepalive

- By default, TCP keepalive is disabled.
- Run the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command to in global configuration mode to enable TCP keepalive. See **Configuration** for parameter description.

In version 10.x, the configuration applies to only IPv4 TCP. In version 11.0 or later, it applies to both IPv4 TCP and IPv6 TCP.

The **service tcp-keepalives-in** command is used in version 10.x to enable keeplive on the TCP server. It is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command.

The **service tcp-keepalives-out** command is used in version 10.x to enable keeplive on the TCP client. It is disused but compatible in version 11.0. If this command is executed, it will be converted to the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command.

This command applies to both TCP server and client.

11.4 Configuration

Configuration	Description and Command	
Optimizing TCP Performance	(Optional) It is used to optimize TCP connection performance.	
	ip tcp synwait-time	Configures a timeout for TCP connection.
	ip tcp window-size	Configures a TCP window size.
	ip tcp send-reset	Configures the sending of TCP reset packets after receiving port unreachable messages.
	ip tcp mss	Configures an MSS for TCP connection.
	ip tcp adjust-mss	Configures an MSS value for the TCPv4 SYN packets
	ipv6 tcp adjust-mss	Configures an MSS value for TCPv6 SYN packets.
	ip tcp path-mtu-discovery	Enables Path MTU Discovery.
Detecting TCP Connection Exception	(Optional) It is used to detect whether the peer works normally.	
	ip tcp keepalive	Enables TCP keepalive.

11.4.1 Optimizing TCP Performance

Configuration Effect

- Ensure optimal TCP performance and prevent fragmentation.

Notes

N/A

Configuration Steps

Configuring SYN Timeout

- Optional.
- Configure this on the both ends of TCP connection.

Configuring TCP Window Size

- Optional.
- Configure this on the both ends of TCP connection.

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages.

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS

- Optional.
- Configure this on the both ends of TCP connection.

Configuring MSS Value for TCPv4 SYN Packets

- Optional.
- If the MTU between two routers in TCP transmission is small, you may configure an MSS value on the routers.

Configuring MSS Value for TCPv6 SYN Packets

- Optional.
- If the MTU between two routers in TCPv6 transmission is small, you may configure an MSS value on the routers.

Enabling Path MTU Discovery

- Optional.
- Configure this on the both ends of TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	**ip tcp synwait-time** *seconds*
Parameter Description	*seconds*: Indicates SYN packet timeout. It ranges from 5 to 300 seconds. The default is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening SYN timeout reduces resource consumption. However, it does not work in continuous SYN flooding. When a device actively makes a request for a connection with an external device, through telnet for example, shortening SYN timeout reduces user's wait time. You may prolong SYN timeout properly on a poor network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size. It ranges from 128 to (65535 << 14) bytes. The default is 65535 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Sending of TCP Reset Packets After Receiving Port Unreachable Messages

Command	**ip tcp send-reset**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, TCP reset packet sending upon receiving port unreachable messages is enabled.

Configuring MSS

Command	**ip tcp mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size. It ranges from 68 to 10000 bytes. By default, the MSS is calculated based on MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP communication to be established. The negotiated MSS for a new connection should be smaller than this MSS. If you want to reduce the MSS, run this command. Otherwise, do not perform the configuration.

Configuring MSS Value for TCPv4 SYN Packets

Command	**ip tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size, ranging from 500 to 1460 bytes
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring MSS Value for TCPv6 SYN Packet

Command	**ipv6 tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: indicates the maximum segment size, ranging from 1220 to 1440 bytes
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring Path MTU Discovery

Command	**ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]
Parameter Description	**age-timer** *minutes*: Indicates the interval for a new probe after a path MTU is discovered. It ranges from 10 to 30 minutes. The default is 10 minutes. **age-timer infinite**: No probe is implemented after a path MTU is discovered.
Command Mode	Global configuration mode
Usage Guide	The PMTUD is an algorithm documented in RFC1191 aimed to improve bandwidth utilization. When the TCP is applied to bulk data transmission, this function may facilitate transmission performance. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The age timer is a time interval for how often TCP estimates the path MTU with a larger MSS. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You may turn off the timer by setting it to **infinite**.

Configuration Example

Enabling Path MTU Discovery

Configuration Steps	Enable PMTUD for a TCP connection. Adopt the default age timer settings.
	`Ruijie# configure terminal` `Ruijie(config)# ip tcp path-mtu-discovery` `Ruijie(config)# end`
Verification	Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.
	`Ruijie# show tcp pmtu` `Number Local Address Foreign Address PMTU` `1 192.168.195.212.23 192.168.195.112.13560 1440`
	Run the **show ipv6 tcp pmtu** command to display the IPv6 TCP PMTU.
	`Ruijie# show ipv6 tcp pmtu` `Number Local Address Foreign Address PMTU` `1 1000::1:23 1000::2.13560 1440`

Common Errors

N/A

11.4.2 Detecting TCP Connection Exception

Configuration Effect

- Check whether the peer works normally.

Notes

N/A

Configuration Steps

↘ Enabling TCP Keepalive

- Optional.

Verification

N/A

Related Commands

↘ Enabling TCP Keepalive

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]
Parameter Description	**interval** *num1*: Indicates the interval to send keepalive packets. Ranging from 1 to120 seconds. The default is 75 seconds. **times** *num2*: Indicates the maximum times for sending keepalive packets. It ranges from 1 to 10. The default is 6. **idle-period** *num3*: Indicates the time when the peer sends no packets to the local end, It ranges from 60 to 1800 seconds. The default is15 minutes.
Command Mode	Global configuration mode
Usage Guide	You may enable TCP keepalive to check whether the peer works normally. The function is disabled by default. Suppose a user enables TCP keepalive function with the default interval, times and idle period settings. The user does not receive packets from the other end within 15 minutes and then starts sending Keepalive packets every 75 seconds for 6 times. If the user receives no TCP packets, the TCP connection is considered inactive and then closed.

Configuration Example

↘ Enabling TCP Keepalive

Configuration Steps	Enable TCP keepalive on a device with **interval** and **idle-period** set to 3 minutes and 60 seconds respectively. If the user receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.

	Ruijie# configure terminal Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180 Ruijie(config)# end
Verification	A user logs in to a device through telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to observe when IPv4 TCP connection is deleted.

Common Errors

N/A

11.5 Monitoring

Displaying

Description	Command
Displays basic information on IPv4 TCP connection.	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP connection statistics.	**show tcp connect statistics**
Displays IPv4 TCP PMTU.	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
Displays IPv4 TCP port information.	**show tcp port** [*num*]
Displays basic information on IPv6 TCP connection.	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP connection statistics.	**show ipv6 tcp connect statistics**
Displays IPv6 TCP PMTU.	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
Displays IPv6 TCP port information.	**show ipv6 tcp port** [*num*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Displays the debugging information on IPv4 TCP packets.	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv4 TCP connection.	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]
Displays the debugging information	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*]

on IPv6 TCP packets.	[**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
Displays the debugging information on IPv6 TCP connection.	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

12 Configuring IPv4/IPv6 REF

12.1 Overview

On products incapable of hardware-based forwarding, IPv4/IPv6 packets are forwarded through the software. To optimize the software-based forwarding performance, Ruijie introduces IPv4/IPv6 express forwarding through software (Ruijie Express Forwarding, namely REF).

REF maintains two tables: forwarding table and adjacency table. The forwarding table is used to store route information. The adjacency table is derived from the ARP table and IPv6 neighbor table, and it contains Layer 2 rewrite(MAC) information for the next hop..

REF is used to actively resolve next hops and implement load balancing.

Protocols and Standards

N/A

12.2 Applications

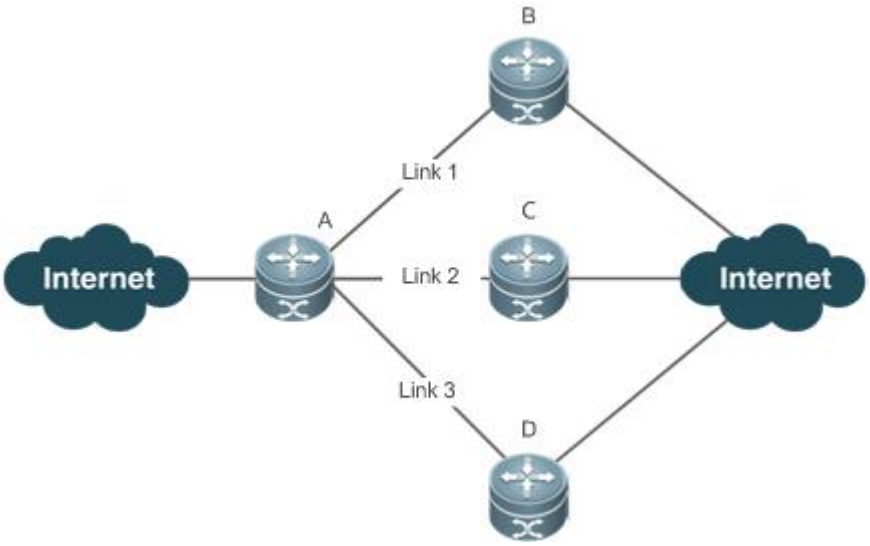
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among the multiple next hops.

12.2.1 Load Balancing

Scenario

As shown in Figure 12-1, a route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3. By default, REF implements load balancing based on the destination IP address. Load balancing can be implemented based on the source IP address and destination IP address as well.

Figure 12-1



Remarks	A is a router that runs REF. B, C and D are forwarding devices.

Deployment

- Run REF on router A.

12.3 Features

Basic Concepts

IPv4/IPv6 REF involves the following basic concepts:

Routing table

An IPv4/IPv6 routing table stores routes to the specific destinations and contains the topology information. During packet forwarding, IPv4/IPv6 REF selects packet transmission paths based on the routing table.

Adjacent node

An adjacent node contains output interface information about routed packets, for example, the next hop, the next component to be processed, and the link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. For the sake of query and update, an adjacent node table is often organized into a hash table. To support routing load balancing, the next hop information is organized into a load balance entry. An adjacent node may not contain next hop information. It may contain indexes of next components (such as other line cards and multi-service cards) to be processed.

Active resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will actively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution while IPv6 REF applies the ND module to resolution.

Packet forwarding path

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined.

12.3.1 Load Balancing Policies

Load balancing is configured to distribute traffic load among multiple network links.

Working Principle

REF supports two load balancing modes. In the REF model, a route prefix is associated with multiple next hops, in other words, it is a multi-path route. The route will be associated with a load balance table and implement weight-based load balancing. When an IPv4/IPv6 packet is matched with a load balance entry based on the longest prefix match, REF performs hash calculation based on the IPv4/IPv6 address of the packet and selects a path to forward the packet.

IPv4/IPv6 REF supports two kinds of load balancing policies: load balancing based on destination IP address, and load balancing based on the source and destination IP addresses.

Related Configuration

Configuring Load Balancing Based on IPv4 Source and Destination Addresses

- By default, load balancing is implemented based on the IPv4 destination addresses.
- Run the **ip ref load-sharing original** command to configure the load balancing.
- After the configuration, load balancing is implemented based on the IPv4 source and destination addresses.

Configuring Load Balancing Based on IPv6 Source and Destination Addresses

- By default, load balancing is implemented based on the IPv6 destination addresses.
- Run the **ipv6 ref load-sharing original** command to configure the load balancing.
- After the configuration, load balancing is implemented based on the IPv6 source and destination addresses.

12.4 Configuration

Configuration	Description and Command	
Configuring Load Balancing Policies	Optional.	
	ip ref load-sharing original	Enables the load balancing algorithm based on IPv4 source and destination addresses.
	ipv6 ref load-sharing original	Enables the load balancing algorithm based on IPv6 source and destination addresses.

12.4.1 Configuring Load Balancing Policies

Configuration Effect

REF supports the following two kinds of load balancing policies:

- Destination address-based load balancing indicates performing hash calculation based on the destination address of the packet. The path with a greater weight is more likely to be selected. This policy is used by default.
- Implementing load balancing based on the source and destination addresses indicates performing hash calculation based on the source and destination addresses of the packet. The path with a greater weight is more likely to be selected.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration if you want to implement load balancing based on the source and destination IP addresses.
- Perform this configuration on a router that connects multiple links.

Verification

Run the **show ip ref adjacency statistic** command to display the IPv4 load balancing policy.

Run the **show ipv6 ref adjacency statistic** command to display the IPv6 load balancing policy.

Related Commands

Configuring Load Balancing Based on IPv4 Source and Destination Addresses

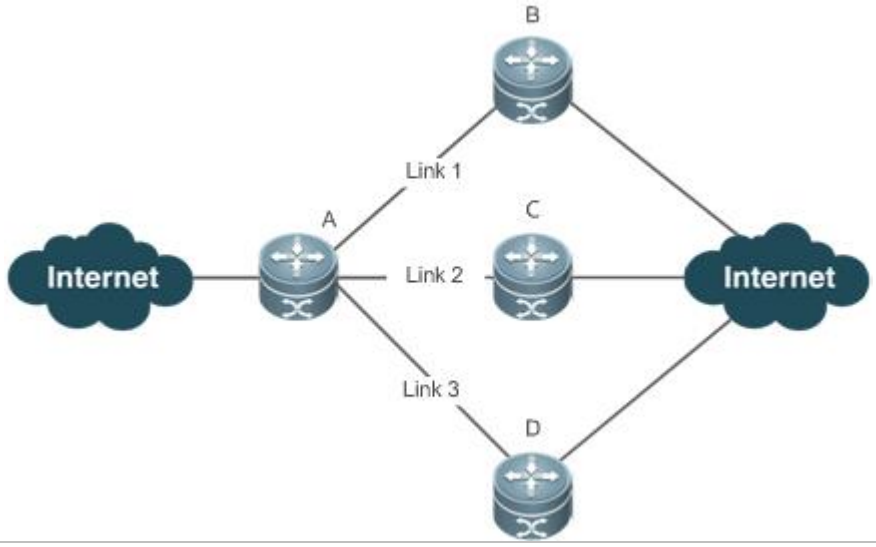
Command	**ip ref load-sharing original**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Load Balancing Based on IPv6 Source and Destination Addresses

Command	**ipv6 ref load-sharing original**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Load Balancing Based on Source and Destination IP Addresses

Scenario **Figure 12-2**	
	A route prefix is associated with three next hops on router A, namely, link 1, link 2, and link 3.
Configuration Steps	Configure load balancing based on IPv4 source and destination IP addresses on router A.
A	A#configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)#ip ref load-sharing original
Verification	
	A #show ip ref adjacency statistics adjacency balance table statistic: source-dest-address load-sharing balance: 0 adjacency node table statistic: total : 3 local : 1 glean : 0 forward: 0 discard: 0 mcast : 1

```
punt   : 1
bcast  : 0
```

12.5 Monitoring

Displaying REF Packet Statistics

REF packet statistics includes the number of forwarded packets and the number of packets discarded due to various causes. You can determine whether packets are forwarded as expected by displaying and clearing REF packet statistics.

Command	Description
show ip ref packet statistics	Displays IPv4 REF packet statistics.
clear ip ref packet statistics	Clears IPv4 REF packet statistics.
show ipv6 ref packet statistics	Displays IPv6 REF packet statistics.
clear ipv6 ref packet statistics	Clears IPv6 REF packet statistics.

Displaying Adjacency Information

You can run the following commands to display adjacency information:

Command	Description
show ip ref adjacency [**glean** | **local** | *ip-address* | {**interface** *interface_type interface_number*) **| discard | statistics**]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.
show ipv6 ref adjacency [glean | local | *ipv6-address* **| (interface** *interface_type interface_number*) **| discard | statistics**]	Displays the gleaned adjacencies, local adjacencies, adjacencies of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes in IPv6 REF.

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved:

Command	Description
show ip ref resolve-list	Displays the next hop to be resolved .
show ipv6 ref resolve-list	Displays the next hop to be resolved.

Displaying Packet Forwarding Path Information

Packets are forwarded based on their IPv4/IPv6 addresses. If the source and destination IPv4/IPv6 addresses of a packet are specified, the forwarding path of this packet is determined. Run the following commands and specify the IPv4/IPv6 source and destination addresses of a packet. The forwarding path of the packet is displayed, for example, the packet is discarded, submitted to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Command	Description
show ip ref exact-route *source-ipaddress dest_ipaddress*	Displays the forwarding path of a packet. oob indicates out-of-band management network.
show ipv6 ref exact-route *src-ipv6-address dst-ipv6-address*	Displays the forwarding path of an IPv6 packet. oob indicates out-of-band, management network.

Displaying Route Information in an REF Table

Run the following commands to display the route information in an REF table:

Command	Description
show ip ref route [**default** | {*ip mask*}| **statistics**]	Displays route information in the IPv4 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.
show ipv6 ref route [**default** | **statistics** | *prefix/len*]	Displays route information in the IPv6 REF table. The parameter **default** indicates a default route. oob indicates out-of-band management network.

13 Configuring TFTP

13.1 Overview

The Trivial File Transfer Protocol (TFTP) service enables a device to be configured as a TFTP server. Then the client can be connected to the TFTP server to upload files to or download files from the device using the TFTP protocol.

Users can easily obtain files such as upgrade package files from the device or copy files to the file system of the device using the TFTP service.

Protocols and Standards

- RFC1350: The TFTP Protocol (revision 2)
- RFC2347: TFTP Option Extension
- RFC2348: TFTP Blocksize Option
- RFC2349: TFTP Timeout Interval and Transfer Size Options

13.2 Applications

Application	Description
Providing the TFTP Service in a LAN	Enables users in a LAN to upload and download files.

13.3 Providing the TFTP Service in a LAN

Scenario

Enable users in a LAN to upload and download files.

In the following figure:

- Device G serves as a TFTP server.
- The User sends a TFTP uploading or downloading request.

Figure 13-1

Remarks G is a network device on which the TFTP server is enabled.

Deployment

- Enable the TFTP server on the device G.
- The user uploads files to or download files from the device G.

13.4 Features

Basic Concepts

TFTP

TFTP is a set of standard protocols defined by the IETF Network Working Group, and operates at the application layer. Implemented on the top of the User Datagram Protocol (UDP), TFTP is a simple protocol to transfer files. TFTP provides only the file uploading and downloading functions instead of many common FTP functions. It does not support the directory list and the authentication function, and does not provide any security mechanism. TFTP uses the way of acknowledged retransmission upon timeout to ensure data transmission, which covers three transmission modes: netascii in the form of an eight-bit ASCII code, eight-bit octet of the source data type, and mail (which is no longer supported). TFTP uses UDP port 69. A description of TFTP can be found in RFC 1350.

TFTP Packet

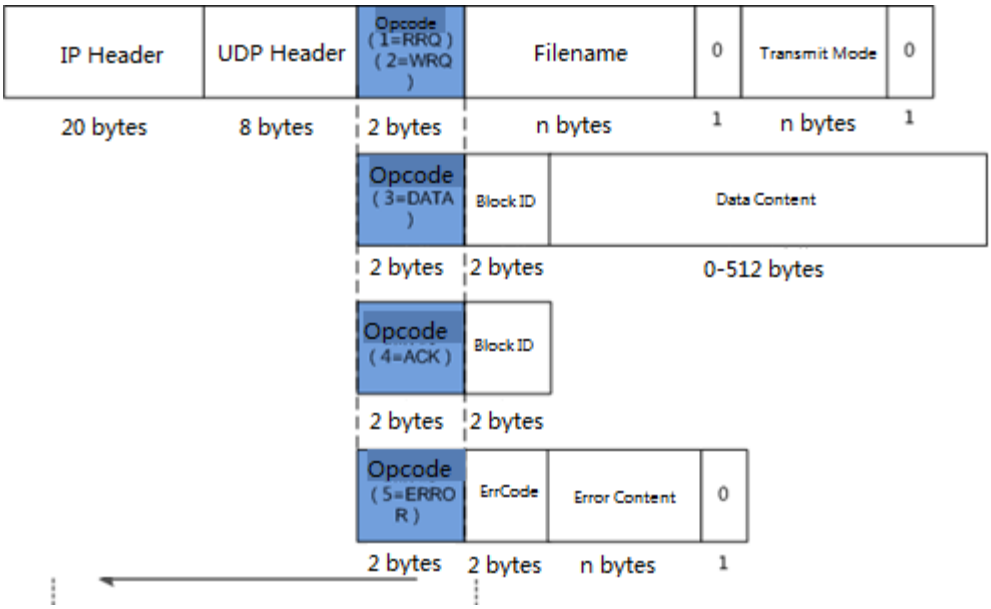
Any transfer begins with a request to read or write a file from a TFTP client. After the TFTP server grants the request, the file is sent in fixed length blocks of 512 bytes. A data packet of less than 512 bytes indicates the termination of a transfer.

Each data packet contains a block of data, and must be acknowledged by an acknowledgement packet before the next data packet can be sent. If no acknowledgement packet is received within specified time, the last sent data packet is retransmitted.

The TFTP packet header includes an opcode field, which indicates the packet type. TFTP supports the following five types of packets:

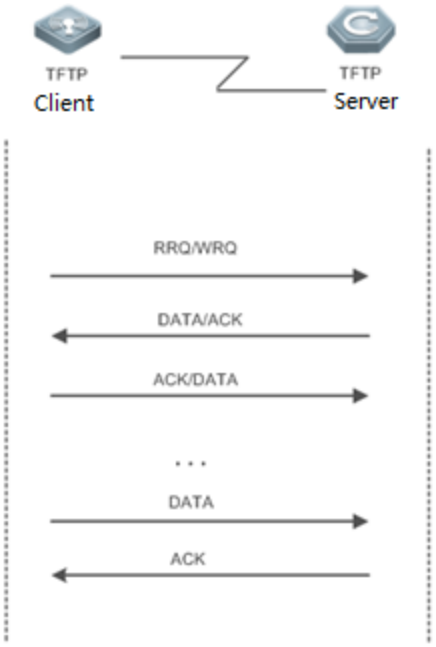
- Read Request (RRQ)
- Write Request (WRQ)
- DATA
- Acknowledgment (ACK)
- ERROR

Figure 13-2



Working Principle

Figure 13-3



- The TFTP client initiates an RRQ or WRQ to the TFTP server.
- Upon receipt of the RRQ, the TFTP server first determines whether the read condition is met (for example, whether the file exists or whether the client has the access permission), and returns a DATA packet to the TFTP client if yes; upon receipt of the WRQ, the TFTP server first determines whether the write condition is met (for example, whether there is a sufficient space or whether the client has the write permission), and returns an ACK packet to the TFTP client if yes.

- The TFTP client receives the DATA packet in the case of file downloading, and replies with an ACK packet; or receives the ACK packet in the case of file uploading, and then sends a DATA packet.
- The process of transmission acknowledgement repeats till the last DATA packet is less than 512 bytes, which indicates the end of the transmission.
- If errors occur during the transmission, an ERROR packet is returned.

13.4.1 Overview

Feature	Description
TFTP Service	Provides the TFTP client with file uploading and downloading functions.

13.4.2 Enabling the TFTP Service

Working Principle

The working principle of TFTP is as described in the previous chapter. After the TFTP service is enabled on the device, configure a top directory so that the TFTP service is available for users.

Related Configuration

Enabling the TFTP Service

- By default, the TFTP service is disabled.
- Run the **tftp-server enable** command to enable the TFTP service.

Configuring the Top Directory

- The default top directory is **flash:**.
- Run the **tftp-server topdir** command to configure the top directory.

13.5 Configuration

Configuration	Description and Command	
Configuring the Basic Functions of the TFTP Service	⚠ Mandatory configuration, which is used to enable the TFTP service.	
	tftp-server enable	Enables the TFTP service.
	tftp-server topdir	Configures the top directory of the TFTP server.

13.5.1 Basic Functions

Networking Requirements

- Establish a TFTP server to provide the TFTP client with uploading and downloading functions.

Configuration Tips

- Top directory configuration is required.

Configuration Steps

↘ Enabling the TFTP Service

- Mandatory configuration.
- Enable the TFTP service on each device unless otherwise stated.

↘ Configuring the Top Directory

- Mandatory configuration.
- Configure a top directory as the root directory on each device unless otherwise stated.

Verification

Connect the TFTP server to the TFTP client.

- Check whether the client is connected to the server.
- Check whether the client can normally download files from and upload files to the server.

Related Commands

↘ Enabling the TFTP Service

Command	**tftp-server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The client cannot access the TFTP server before a top directory is correctly configured for the server. Therefore, it is recommended that you configure the top directory of the server first if it is the first time for you to enable the TFTP server. For details about how to configure the top directory, see the description to immediately follow below.

↘ Configuring the Top Directory of the TFTP Server

Command	**tftp-servertopdir** *directory*
Parameter	*directory*: access path

Description	
Command Mode	Global configuration mode
Usage Guide	For example, you can set the top directory of the server to **/dir**. Then the TFTP client can access files and folders in only the **/dir** directory on the device after logging in, and the TFTP client cannot return to the parent directory of the **/dir** directory due to the restrictions of the top directory.

Enabling the TFTP Server Debugging Switch

Command	**debug tftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can run this command to enable the TFTP server debugging switch, so that the process or error information of the TFTP server can be output as necessary.

Displaying the Completed Update Process

Command	**show tftp-server updating-list**
Parameter Description	N/A
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode
Usage Guide	You can run this command to display the completed update process on the current TFTP client. This command is supported only on RG-AM5528 access points.

Configuration Example

Establishing the TFTP Service on an IPv4 Network

Scenario	● Enable the TFTP service. ● Set the top directory of the TFTP server to /dir.
	`Ruijie(config)#tftp-server topdir /tmp` `Ruijie(config)#tftp-server enable`
Verification	● Run the **show tftp-server** command to display the configuration. `Ruijie#show tftp-server` `...` `tftp-server information` `==========`

	enable : Y topdir : tmp:/

Common Errors

No top directory is configured.

13.6 Monitoring

Displaying

Function	Command
Displays the configuration of the TFTP server.	**show tftp-server**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Function	Command
Enables the TFTP server debugging switch.	**debug tftp-server**
Displays the completed update process.	**show tftp-server updating-list**

14 Configuring NAT

1.1. Overview

Network Address Translation (NAT) is a process of translating the IP address in the header of an IP data packet into another IP address. In practice, NAT enables private networks that use unregistered IP addresses to access public networks. This way of using a small number of public IP addresses to represent substantial private IP addresses implements IP address conservation.

Protocols and Standards

- RFC 1631: The IP Network Address Translator (NAT)
- RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2391: Load Sharing using IP Network Address Translation (LSNAT)
- RFC 4008: Definitions of Managed Objects for Network Address Translators (NAT)

1.2. Applications

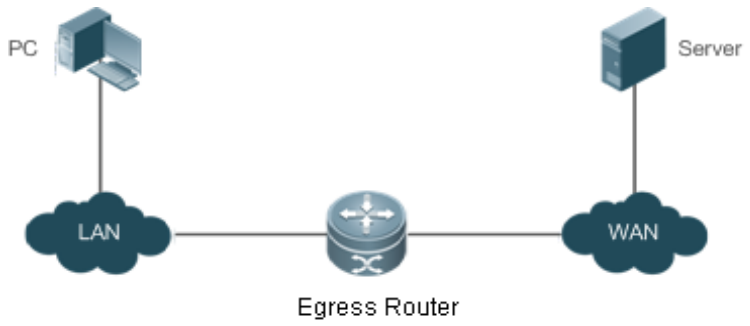
Application	Description
Intranet Users' Access to the Internet	NAT allows an intranet to communicate with the Internet by translating an inside private IP address into a globally unique IP address.
External Users' Access to an Intranet Server	NAT allows external networks to access internal devices by mapping one or more internal hosts to a network server.
Source/Destination Address Translation for Internal Users	When two private networks to interconnect with each other are configured with the same IP address or the same global IP address is allocated to both a private network and a public network, the two network hosts with the same IP address cannot communicate. NAT allows overlapping networks to communicate..
Intranet Server Load Balancing	When the TCP traffic load of an intranet host is excessively heavy, multiple hosts are deployed for TCP service load balancing. In this case, NAT may be used to attain this objective.

1.2.1. Intranet Users' Access to the Internet

Scenario

A PC is located in an intranet while a server is located in an extranet, as shown in Figure 14-1. In view of IP address depletion, only one or a few public IP addresses are allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The basic NAT function is required on the egress router to allow the intranet PC to access the extranet server.

Figure 14-1



The egress router connects both the intranet and the extranet.

Corresponding Protocols

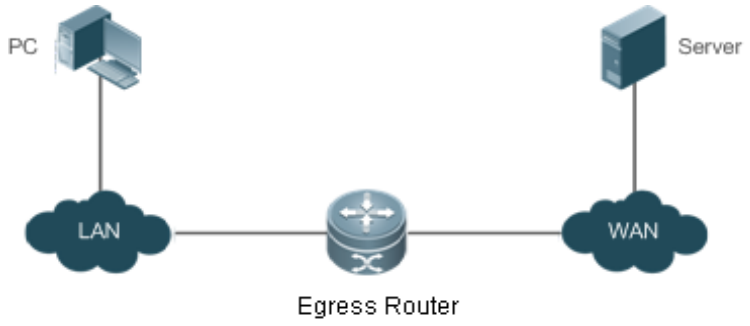
- Configure an inside interface and an outside interface for NAT.
- Configure static inside source address translation on the egress router.

1.2.2. External Users' Access to an Intranet Server

Scenario

A PC is located in an extranet while a server (such as a Web server) is located in an intranet, as shown in Figure 14-2. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The Network Address and Port Translation (NAPT) function is required on the egress router to enable the PC to access the intranet server; that is, port mapping applies to the Web service port.

Figure 14-2



The egress router connects both the intranet and the extranet.
The server is deployed in the intranet.

Corresponding Protocols

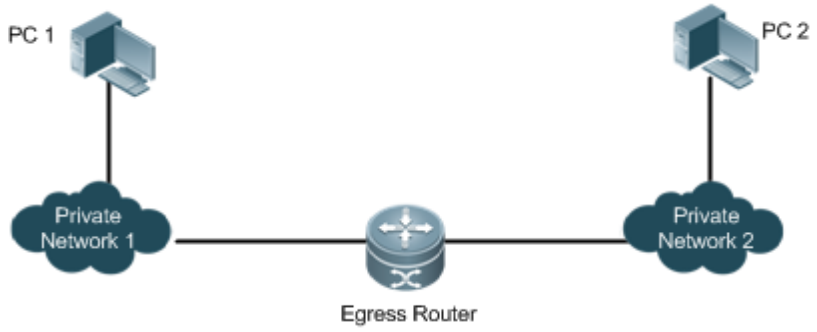
- Configure an inside interface and an outside interface for NAT.
- Configure server port address translation rules on the egress router.

1.2.3. Source/Destination Address Translation for Internal Users

Scenario

PC 1 is located in private network 1 while PC 2 is located in private network 2, as shown in Figure 14-3. Because the two private networks are separately managed, address overlapping occurs in their IP network segments. For example, the IP addresses of PC 1 and PC 2 are configured in the same network segment 192.168.1.0/24. An egress router is located between private networks 1 and 2. The NAT function needs to be enabled on the egress router, so that PC 1 and PC 2 can access each other.

Figure 14-3



The egress router connects both private networks.

Corresponding Protocols

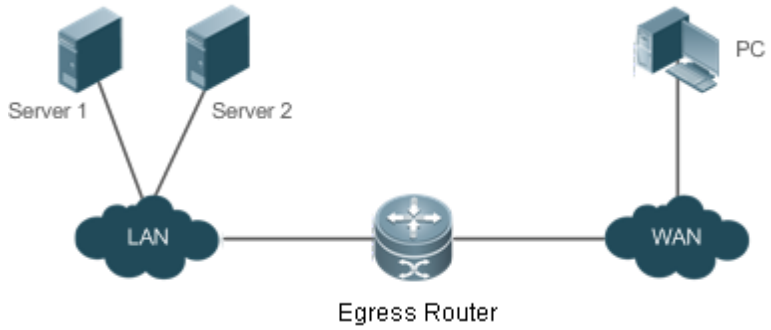
- Configure an inside interface and an outside interface for NAT.
- Configure dynamic translation of the inside source address on the egress router.
- Configure dynamic translation of the outside source address on the egress router.

1.2.4. Intranet Server Load Balancing

Scenario

Server 1 and Server 2 are located in an intranet, and form a cluster, as shown in Figure 14-4. A PC is located in an extranet. In view of IP address depletion, only one public IP address is allocated to the entire campus network. An egress router belongs to the intranet, and connects to the extranet. The egress router needs to distribute the server access traffic of the external user to the two servers; therefore, the NAT load balancing function needs to be enabled on the egress router.

Figure 14-4



The egress router connects both the intranet and the extranet.
The servers are deployed in the intranet.

Corresponding Protocols

- Configure an inside interface and an outside interface for NAT.
- Configure TCP load balancing using NAT on the egress router.

1.3. Features

Basic Concepts

Private Address and Public Address

A private address is the IP address of an intranet or an intranet host, whereas a public address is an IP address globally unique on the Internet. The Internet Assigned Numbers Authority (IANA) has stipulated the following IP addresses for use on private networks, which cannot be allocated for use on the Internet but can be used inside any institution or corporation.

Class A private addresses: 10.0.0.0 to 10.255.255.255

Class B private addresses: 172.16.0.0 to 172.31.255.255

Class C private addresses: 192.168.0.0 to 192.168.255.255

NAT was initially designed to enable a private network to access a public network. Later it was extended to implement address translation for mutual access between any two networks. In this document, the two networks are called an intranet and an extranet. In general, a private network is an intranet, and a public network is an extranet.

Static NAT

Static NAT allows one-to-one permanent mappings between inside local addresses and inside global addresses. Static NAT is important when an extranet needs to access internal hosts via a fixed global routable address.

Dynamic NAT

Dynamic NAT establishes temporary mapping relationships between inside local addresses and inside global addresses. The temporary mapping relationships will be removed when unused in a certain period of time. Dynamic NAT can be

configured in the following case: An intranet accesses extranet services only but does not provide services, and the number of intranet hosts is greater than the number of global IP addresses.

Overview

Feature	Description
Basic NAT	This feature translates inside private addresses into globally unique addresses, so that the intranet and the public network can communicate with each other.
NAPT	This feature maps multiple inside local addresses to one inside global address, so as to resolve the problem of IP address depletion.
Overlapping NAT	This feature enables overlapping networks to communicate.
TCP Load Balancing	This feature resolves the problem of TCP traffic overload.
Constructing a Local Server	This feature enables extranet to access the local server.
ALG	NAT changes only the header of an IP packet but not the payload of a specific application protocol. Therefore, the Application Level Gateway (ALG) is introduced to support application layer protocols.

1.3.1. Basic NAT

NAT is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Working Principle

An IP packet sent by an intranet host (192.168.1.2) to an extranet server (8.8.8.8) reaches an NAT device.

The NAT device checks the content of the IP packet, and finds that the IP packet is destined to an extranet. Therefore, the NAT device translates the private IP address 192.168.1.2 in the source IP address field of the IP packet into a public IP address 30.1.1.1 routable on the Internet, sends the IP packet to the extranet server, and at the same time records the mapping in its own NAT table.

The extranet server returns a response packet (in which the initial destination IP address is 30.1.1.1) to the intranet user. When the response packet reaches the NAT device, the NAT device checks the content of the response packet, looks up the mapping record in the NAT table, and replaces the initial destination IP address with the inside private IP address 192.168.1.2.

The above NAT process is transparent to terminals, such as the host and the server shown in the preceding figures. In the point of view of the extranet server, the IP address of the intranet host is 30.1.1.1 and the extranet server itself does not know the existence of the IP address 192.168.1.2 at all. Therefore, NAT "hides" the private network of an enterprise.

Basic NAT includes static NAT and dynamic NAT.

Related Configuration

↘ Configuring NAT Interfaces

- An interface is not an NAT interface by default.

- Use the **ip nat { inside | outside }** command to configure the interfaces as connected to the inside and outside.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAT

- Static NAT is not configured by default.
- Use the **ip nat inside source static** local-address global-address [**permit-inside**] [**netmask** mask] [**match** interface] command to configure static one-to-one NAT mapping.

Configuring Dynamic NAT

- Dynamic NAT is not configured by default.
- Use the **ip nat inside source list** access-list-number **pool** address-pool command to configure dynamic NAT mapping.

1.3.2. NAPT

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

Working Principle

NAPT, also known as multiple-to-one address translation, allows multiple inside addresses to map to one public address. NAPT maps both IP addresses and port numbers; that is, the source addresses of data packets from different inside addresses can map to the same public address, but their port numbers are translated into different port numbers of the public address so that the same address can still be shared. NAPT is translation between "private IP address + Port number" and "Public IP address + Port number".

Static NAPT

In general, static NAPT is used to map the specified port on a specified host in an intranet to the specified port of a global address. In comparison, as mentioned previously, static NAT maps an internal host to a global address. Static NAPT is applicable to intranet hosts that provide the information service. Static NAPT provides a permanent one-to-one "IP address + Port" mapping relationship.

Dynamic NAPT

Dynamic NAPT is applicable to intranet hosts that only access extranet services but do not provide any information service. Dynamic NAPT provides a temporary one-to-one "IP address + Port" mapping relationship.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- Use the **ip nat { inside | outside }** command to configure the interfaces as connected to the inside and outside.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Static NAPT

- Static NAPT is not configured by default.
- Use the **ip nat inside source static** local-ip **interface** *interface* [permit-inside] command to configure static one-to-one NAPT mapping.

Configuring Dynamic NAPT

- Dynamic NAPT is not configured by default.
- Use the **ip nat inside source list** access-list-number { [**pool** address-pool] | [**interface** interface-type interface-number] } **overload** command to configure dynamic NAPT mapping. For NAPT, generally only one IP address is defined in the address pool, and one IP address supports up to 64,512 times of NAT. If one IP address is not enough, multiple IP addresses can be defined in the address pool.

1.3.3. Overlapping NAT

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Working Principle

For mutual access between an intranet and an extranet with the same IP address, NAT needs to translate the inside address into a unique outside address. In addition, NAT needs to translate the outside address that overlaps with the inside address into another unique inside address.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- Use the **ip nat { inside | outside }** command to configure the interfaces as connected to the inside and outside.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Inside Source Address Translation

- Inside source address translation is not configured by default.
- Static/dynamic basic NAT or static/dynamic NAPT can be used for inside source address translation. For details, see the "Basic NAT" and "NAPT" sections.

Configuring Static Translation of Outside Source Address

- Static translation of outside source address is not configured by default.
- Use the **ip nat outside source static** *global-address local-address* command to configure static translation of outside source address.

Configuring Dynamic Translation of Outside Source Address

- Dynamic translation of outside source address is not configured by default.
- Use the **ip nat outside source list** *access-list-number* **pool** *address-pool* command to configure dynamic translation of outside source address.

Configuring an ACL

- No ACL is configured by default.
- Use the **ip access-list { extended | standard } {** *id* | *name* **}** command or the **access-list** command to configure an ACL.

Configuring a Static Route

- Mandatory configuration.
- Use the **ip route** *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**] command to configure a static route, which is used to specify the network egress after inside destination address translation.

1.3.4. TCP Load Balancing

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective.

Working Principle

Create a virtual host with NAT to provide the TCP service. The virtual host maps to multiple physical hosts. Then the virtual host polls and replaces destination addresses, so as to implement traffic load distribution.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- Use the **ip nat** { **inside | outside** } command to configure the interfaces as connected to the inside and outside.

- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring the Address Pool

- No address pool is configured by default.
- Use the **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* } command to configure an IP address pool for NAT.

Configuring the ACL

- No ACL is configured by default.
- Use the **access-list** *access-list-number* **permit** *ip-address wildcard* command to configure a destination-based ACL. Note that the ACL must be configured as an extended ACL based on destination IP address matching.

Configuring Inside Destination Address Translation

- Inside destination address translation is not configured by default.
- Use the **ip nat inside destination list** *access-list-number* **pool** *address-pool* command to configure inside destination address translation. This configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

1.3.5. Constructing a Local Server

A user has deployed three servers (an FTP server, a Web server, and an Email server) in an intranet, and hopes that network hosts in a WAN can access the three servers while common users of the intranet can set the gateway as a device to provide Internet access.

Working Principle

Map one or more internal hosts to a network server, so that users on the WAN obtain corresponding services from the network server.

Related Configuration

Configuring NAT Interfaces

- An interface is not an NAT interface by default.
- Use the **ip nat** { **inside | outside** } command to configure the interfaces as connected to the inside and outside.
- NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured.

Configuring Inside Address and Port Translation

- Inside address and port translation is not configured by default.

- Use the **ip nat inside source static** { **udp** | **tcp** } **local-address port global-address port** [**permit-inside**] command to translate specific inside addresses and ports, so that corresponding services are provided on dedicated ports. For example, TCP port 20 or 21 can be used to construct an FTP server, or TCP port 80 to construct a Web server.

1.3.6. ALG

Common NAT can translate the IP address and port in the header of a UDP or TCP packet, but is helpless before fields in application layer data payloads. In many application layer protocols such as multimedia protocols (H.323 and the like), FTP, and SQLNET, the TCP/UDP payload carries address or port information. If such address or port information cannot be translated by NAT, problems may occur.

Working Principle

The ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications. All types of ALGs are enabled for NAT by default. Currently the protocols that support ALG include DNS, FTP, H323, PPTP, TFTP, RTSP, and SIP.

Related Configuration

↘ Enabling or Disabling ALG

- By default, all ALGs are enabled.
- Use the **no ip nat translation dns** command to disable DNS ALG.
- Use the **no ip nat translation ftp** command to disable FTP ALG.
- Use the **no ip nat translation h323** command to disable H323 ALG.
- Use the **no ip nat translation pptp** command to disable PPTP ALG.
- Use the **no ip nat translation tftp** command to disable TFTP ALG.
- Use the **no ip nat translation rtsp** command to disable RTSP ALG.

1.4. Configuration

Configuration	Description and Command	
Configuring Basic NAT	⚠ Mandatory configuration. It is used to configure one-to-one NAT for internal PCs to connect to a WAN.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	⚠ Optional configuration. It is used to configure static NAT.	

	ip nat inside source static *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** interface]	Defines the static inside source address translation relationship.
	⚠ Optional configuration. It is used to configure dynamic NAT.	
	ip nat pool address-pool start-address end-address { **netmask** mask | **prefix-length** prefix-length } or **ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] **address** *start-ip end-ip* [**match interface** *interface*]	Defines a global IP address pool. For NAT, generally multiple IP addresses are defined. The number of address pools to be defined shall depend on the number of intranet users.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration .
Configuring NAPT	⚠ Mandatory configuration. It is used to configure NAPT.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside.
	⚠ Optional configuration. It is used to configure static NAPT.	
	ip nat inside source static { **UDP** *local-address port* | **TCP** *local-address port* } *global-address port* [**permit-inside**]	Defines the static inside source address translation relationship.
	⚠ Optional configuration. It is used to configure dynamic NAPT.	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines a global IP address pool. For NAPT, generally only one IP address is defined.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.

	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring Overlapping NAT	Mandatory configuration. It is used to enable overlapping networks to communicate using NAT.	
	ip nat inside	Marks the interface as connected to the inside.
	ip nat outside	Marks the interface as connected to the outside..
	ip nat inside source static *local-address global-address*	Configures inside source address translation.
	⚠ Optional configuration. It is used to configure static NAT.	
	ip nat outside source static *global-address local-address*	Configures static NAT.
	⚠ Optional configuration. It is used to configure dynamic NAT.	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines a global IP address pool.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, so that only the addresses matching this ACL are translated.
	ip nat outside source list *access-list-number* **pool** *address-pool*	Defines the dynamic source address translation relationship. The *overload* parameter may be omitted. It is used only to keep compatibility with mainstream vendors' configuration.
Configuring TCP Load Balancing	⚠ Mandatory configuration. It is used to configure destination address polling and translation.	
	ip nat inside	Marks the interface as connected to inside.
	ip nat outside	Marks the interface as connected to outside.
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	Defines an IP address pool, which includes all physical host addresses.

	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL, which matches the virtual host address only. ⚠ Ensure that the ACL is an extended ACL based on destination IP address matching.
	ip nat inside destination list *access-list-number* **pool** *address-pool* [**vrf** vrf_*name*]	Defines the dynamic inside destination address translation relationship.
Configuring ALG	⚠ Optional configuration. It is used to configure ALG for relevant protocols.	
	ip nat translation { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **tftp** | **pptp** | **h323** | **rtsp** | **sip** }	Defines ALG for relevant protocols.
Configuring Special NAT Applications	⚠ Optional configuration. It is used to configure special NAT applications.	
	ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }	Defines rules for special NAT applications.
Configuring the Interval at Which NAT Sends Gratuitous ARP Packets	⚠ Optional configuration. It is used to configure the interval at which gratuitous ARP packets are sent from the local address of NAT.	
	ip nat keepalive [*keealive_out*]	Defines the interval at which gratuitous ARP packets are sent from the local address of NAT.

1.4.1. Configuring Basic NAT

Networking Requirements

NAT configuration is required for an intranet to communicate with an extranet by translating an inside private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection and interworking.

Notes

- At least one inside interface and one outside interface need to be configured for basic NAT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.

Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

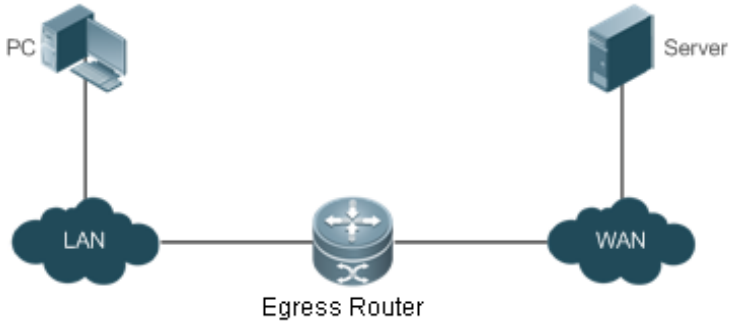
Command	**ip nat pool** address-pool start-address end-address { **netmask** mask | **prefix-length** prefix-length }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Enabling Intranet Users to Access an Extranet Server

Scenario **Figure 14-5**	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAT rule.

A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Verification	Use the **show** command to display the configuration.
A	Ruijie# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.2. Configuring NAPT

Networking Requirements

In general, traditional NAT is one-to-one address mapping, which, however, cannot meet the requirements of all hosts in intranets to communicate with extranets. For example, when the intranet is in short of global IP addresses or even does not apply for global IP addresses but has only one global IP address to connect to an Internet Service Provider (ISP) while a large number of hosts in the intranet need to access the Internet, NAPT is required in this scenario.

Multiple inside local addresses can map to one inside global address using NAPT.

Notes

- At least one inside interface and one outside interface need to be configured for NAPT.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAPT

- Optional configuration.
- Configure static NAPT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAPT

- Optional configuration.
- Configure dynamic NAPT in global configuration mode when a large number of users in the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAPT

Command	**ip nat inside source static** { **udp** *local-address port* | **tcp** *local-address port* } *global-address port* [**permit-inside**]
Parameter Description	**udp**: UDP **tcp**: TCP *local-address*: inside local address

	port: inside local port *global-address*: outside global address *port*: outside global port **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*.
Command Mode	Global configuration mode
Configuration Usage	This command is used to build an internal server that external public networks can access. Internal hosts are not allowed to access the internal server using the *global-address* unless **permit-inside** has been configured. If **permit-inside** is not configured, internal hosts can access the internal server by using the *local-address* only.

Configuring the Address Pool

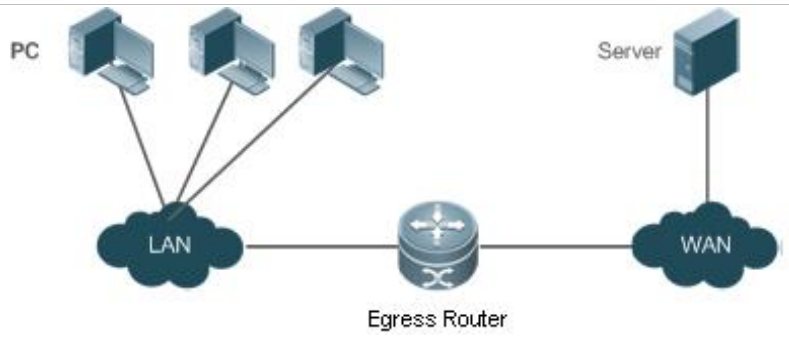
Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAPT

Command	**ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool **interface** *interface-type interface-number*: implements NAPT using the global address of the outside interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. Currently, the global addresses are reused even if this parameter is not configured. Therefore, this parameter is used only to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	-

Configuration Example

Enabling Intranet User to Access an Extranet Server Through NAPT

Scenario **Figure 14-6**	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAPT rule.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.1 200.168.12.1 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
Verification	Use the **show** command to display the configuration.
A	Ruijie# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23 icmp 200.168.12.200:2064 192.168.12.66:2063 168.168.12.1:23 168.168.12.1:23 udp 200.168.12.200:2065 192.168.12.67:2063 168.168.12.1:23 168.168.12.1:23 tcp 200.168.12.200:2066 192.168.12.68:2063 168.168.12.1:23 168.168.12.1:23

	tcp 200.168.12.200:2067 192.168.12.69:2063 168.168.12.1:23 168.168.12.1:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.3. Configuring Overlapping NAT

Networking Requirements

When the same IP address is allocated to two private networks to interconnect with each other or the same global IP address is allocated to a private network and a public network, this situation is called address overlapping. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is in the local network. Overlapping NAT is especially designed to implement the communications between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address in the intranet, and vice versa.

Notes

- Internal source address translation must be configured before overlapping NAT is configured.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static Translation of Outside Source Address

- Optional configuration.
- Configure static translation of outside source address in global configuration mode when a small number of users in the extranet need to access the intranet.

Configuring Dynamic Translation of Outside Source Address

- Optional configuration.
- Configure dynamic translation of outside source address in global configuration mode when a large number of users in the extranet need to access the intranet.

Configuring an ACL

- ACL configuration is mandatory when dynamic source address mapping is used.
- Restrict the range of users requiring source address translation in the intranet.

Configuring a Static Route

- Mandatory configuration.
- Specify the network egress after inside destination address translation.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static Translation of Outside Source Address

Command	**ip nat outside source static** *global-address local-address*
Parameter Description	*global-address*: outside global address *local-address*: inside local address
Command Mode	Global configuration mode
Configuration Usage	

Configuring Static Translation of Outside Source Address and Port

Command	**ip nat outside source static** { **tcp** *global-address global-port* **| udp** *global-address global-port* } *local-address local-port*
Parameter Description	*protocol*: protocol number *global-address*: outside global address *global-port*: outside global port *local-address*: inside local address *local-port*: inside local port
Command Mode	Global configuration mode
Configuration	-

Usage	

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	--

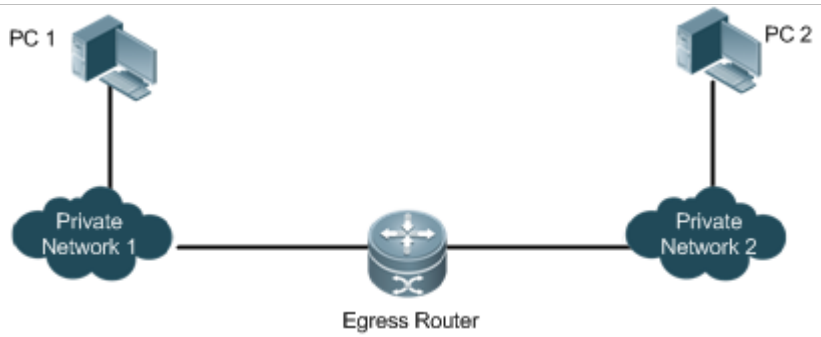
Configuring Dynamic Translation of Outside Source Address

Command	**ip nat outside source list** *access-list-number* **pool** *pool-name*
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

The following configuration example describes configuration related to static translation of outside source address.

Static Translation of Outside Source Address

Scenario **Figure 14-7**	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a rule for dynamic translation of inside source address.

	● Configure a rule for static translation of outside source address.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat outside source static 192.168.12.3 172.16.10.1 A(config)# ip route 172.16.10.0 255.255.255.0 200.198.12.2
Verification	Use the **show** command to display the configuration.
A	Ruijie# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 200.168.12.200:2063 192.168.12.65:2063 172.16.10.1:23 168.168.12.3:23

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.
- No static route is configured or no IP address is configured for the outside interface, so that the router does not know to which interface a data packet should be sent after NAT or from which interface a data packet is received after NAT.

1.4.4. Configuring TCP Load Balancing

Networking Requirements

When the TCP traffic load of an intranet host is excessively heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to attain this objective. In the following configuration, a virtual host address is defined, so that all TCP connections from extranets to the virtual host are distributed by a router to multiple physical hosts, so as to implement traffic load balancing.

Notes

The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Dynamic Translation of Inside Destination Address

- Mandatory configuration.
- Configure dynamic translation of inside destination address in global configuration mode for TCP load balancing.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring the Address Pool

Command	**ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

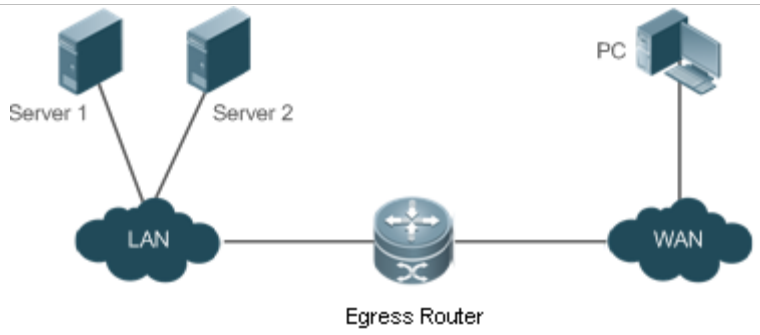
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses **type rotary**: NAT address pool type. Rotary type guarantees equal chance of every address to be assigned. Whether **type rotary** is configured or not, the NAT address pool type is rotary. This parameter is introduced for compatibility with Cisco.
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic Translation of Inside Destination Address

Command	**ip nat inside destination list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *pool-name*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Enabling Extranet User to Access an Intranet Server

Scenario Figure 14-8	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a rule for dynamic inside destination address translation.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/0`

	A(config-if-GigabitEthernet 0/0)# ip address 10.10.10.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary A(config)# ip nat inside destination list 100 pool realhosts A(config)# access-list 100 permit ip any host 10.10.10.100
Verification	Use the **show** command to display the configuration.
A	Ruijie# show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 10.10.10.100:23 10.10.10.2:23 100.100.100.100:1178 100.100.100.100:1178 tcp 10.10.10.100:23 10.10.10.3:23 200.200.200.200:1024 200.200.200.200:1024

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect. Note that the ACL must be configured as an extended ACL based on destination IP address matching.
- The above configuration takes effect on TCP traffic only but not on other traffic, unless additional NAT configuration has been performed.

1.4.5. Configuring ALG

Networking Requirements

In general, NAT translates only IP address and port information in the header of a packet but does not analyze fields in the application layer data payload of the packet. However, for some special protocols, such as FTP, DNS, and FTFP, the data payloads of their packets may contain IP address or port information. If such information is not translated by NAT, certain problems may occur. The NAT ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process the IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing the correctness of application layer communications.

Notes

- At least one inside interface and one outside interface need to be configured during the configuration of ALG.

- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring ALG

- Optional configuration.
- The ALG configuration is mandatory if the DNS, FTP, TFTP, PPTP, H323, RTSP, or SIP protocol in the environment needs to implement NAT transversal for communications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

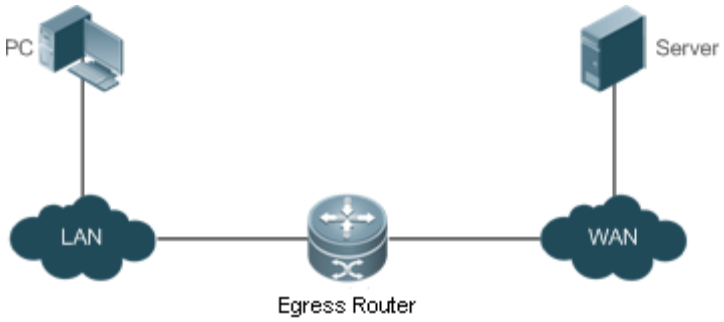
Configuring ALG

Command	**ip nat translation** { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **tftp** | **pptp** | **h323** | **rtsp** | **sip** }
Parameter Description	**ttl**: defines the NAT timeout interval of the UDP connection of the DNS application. The default value is 0. *port_num*: defines the port number used for the FTP application. The default value is 21.
Command Mode	Global configuration mode

Configuration Usage	

Configuration Example

Enabling Intranet Users to Access an Extranet Server

Scenario Figure 14-9	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAT rule. ● Configure ALG.
A	A# configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat translation ftp 23
Verification	Use the **show** command to display the configuration.
A	Ruijie# show ip nat translations

```
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

Common Errors

- The inside or outside interface is not configured.
- The ACL configuration is incorrect.

1.4.6. Configuring Special NAT Applications

Networking Requirements

For some advanced applications of NAT, the source addresses or destination addresses of some specific IP packets need to be modified.

Notes

- At least one inside interface and one outside interface need to be configured for special NAT applications.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Steps

Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring Special NAT Applications

- Optional configuration.

- This configuration is mandatory if special address translation is required for the communications of some applications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
CommandMode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	

Configuring Dynamic NAT

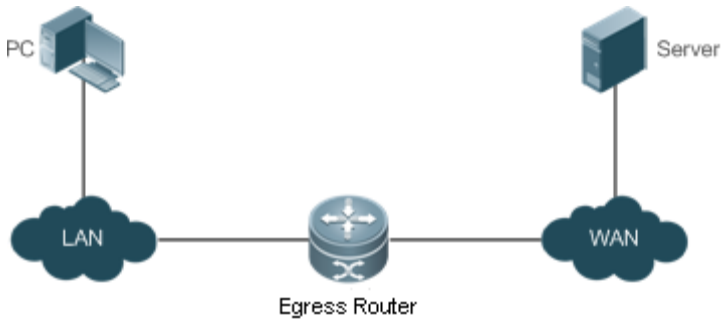
Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	

Configuring Special NAT Applications

Command	**ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration Usage	

Configuration Example

Implementing the DNS Relay Service

Scenario Figure 14-10	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAT rule. ● Configure special NAT applications.
A	`A#configure terminal` `A(config)# interface GigabitEthernet 0/0` `A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0`

	A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1.)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55 53 A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Verification	

Common Errors

- The inside or outside interface is not configured.

1.4.7. Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Networking Requirements

Configure the interval at which gratuitous ARP packets are sent from addresses in the NAT address pool, so as to avoid address conflicts.

Notes

- Sending gratuitous ARP packets is disabled by default on the NAT device.
- Gratuitous ARP packets are sent to the outside interface only.

Configuration Steps

↘ Configuring the NAT Inside Interface

- Mandatory configuration.
- Configure the LAN interface to connect to the intranet as the NAT inside interface unless otherwise stated.

↘ Configuring the NAT Outside Interface

- Mandatory configuration.
- Configure the WAN interface to connect to the extranet as the NAT outside interface unless otherwise stated.

Configuring Static NAT

- Optional configuration.
- Configure static NAT in global configuration mode when a small number of users in the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional configuration.
- Configure dynamic NAT in global configuration mode when a large number of users in the intranet need to access the extranet.

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

- Optional configuration.
- NAT needs to consider some addresses matching the configured rule as local addresses. This configuration is performed to avoid address conflicts.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: inside interface **outside**: outside interface
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the outside interface and the inside interface and the data packet meets a certain rule. Therefore, at least one inside interface and one outside interface need to be configured on the router.

Configuring Static NAT

Command	**ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]
Parameter Description	*local-address*: inside address *global-address*: outside address **permit-inside**: permits intranet users to access the *local-ip* host using *global-ip*. **netmask** *mask*: network-segment-to-network-segment address **match** *interface*: specifies the egress interface.
Command Mode	Global configuration mode
Configuration	

Usage	

Configuring the Address Pool

Command	**ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }
Parameter Description	*address-pool*: name of the address pool *start-address*: start IP address *end-address*: end IP address **netmask** *mask*: network mask of the addresses **prefix-length** *prefix-length*: length of the network mask of the addresses
Command Mode	Global configuration mode
Configuration Usage	-

Configuring Dynamic NAT

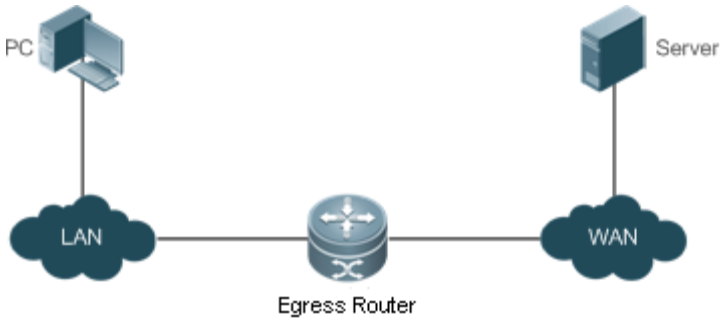
Command	**ip nat inside source list** *access-list-number* **pool** *address-pool*
Parameter Description	*access-list-number*: ACL number **pool** *address-pool*: name of the address pool
Command Mode	Global configuration mode
Configuration Usage	-

Configuring the Interval at Which NAT Sends Gratuitous ARP Packets

Command	**ip nat keepalive** [*keealive_out*]
Parameter Description	*keealive_out*: the interval at which gratuitous ARP packets are sent from the local address of NAT.
Command Mode	Global configuration mode
Configuration Usage	-

Configuration Example

Implementing the Sending of Gratuitous ARP Packets regularly

Scenario **Figure 14-11**	
Configuration Steps	● Configure **ip nat inside** on the inside interface. ● Configure **ip nat outside** on the outside interface. ● Configure a dynamic NAT rule. ● Configure the periodical sending of gratuitous ARP packets.
A	A#configure terminal A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/0)# ip nat inside A(config-if-GigabitEthernet 0/0)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)# ip nat outside A(config-if-GigabitEthernet 0/1.)# exit A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 A(config)# ip nat inside source list 1 pool net200 A(config)# access-list 1 permit 192.168.12.0 0.0.0.255 A(config)# ip nat keepalive 10
Verification	-

Common Errors

- The inside or outside interface is not configured.
- NAT rule is not correct.

1.5. Monitoring

Displaying

Function	Command
Displays NAT records.	**show ip nat translations** [*dv_id*] [*slot_id*] [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

15 Configuring ARP Proxy

15.1 Overview

ARP Proxy is a feature of Ruijie AC (access controller, a wireless controller) product. It can work as a proxy for a device in the wireless local area network (WLAN) to respond to ARP requests of another device. Because CSMA/CA is used for communication in a wireless network, ARP Proxy can prevent ARP broadcast packets in one access point (AP) from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Protocols and Standards

N/A

15.2 Applications

Application	Description
ARP Proxy Service in the WLAN	AC acts as a proxy to respond to ARP requests of any device in the WLAN.

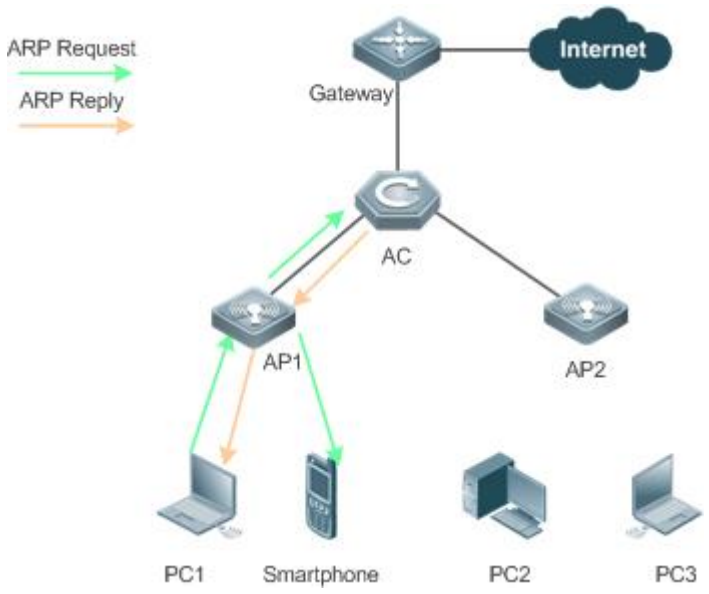
15.2.1 ARP Proxy Service in the WLAN

Scenario

In centralized forwarding mode of the fit AP, AC acts a proxy for ARP requests of any device in the WLAN.

- The AC needs to learn the MAC address of devices in the WLAN before responding to this device.

Figure 15-1



Remarks	The above figure is the flowchart of the ARP request packets that wireless STAs send to the gateway or other devices in centralized forwarding mode of the fit AP in the WLAN.

Deployment

- Deploy a network consisting of the gateway, AC, APs, and wireless STAs. Using the ARP Proxy function (enabled by default), AC works as a proxy to respond to the ARP requests of wireless STAs to prevent the ARP broadcast requests from being sent to other APs.
- The ARP Proxy runs on AC and is transparent to users. You can run this function without any other configurations. For details about how to deploy the network environment, refer to the chapter related to wireless networking.

15.3 Features

Basic Concepts

↘ ARP Proxy

Layer-2 ARP Proxy is a feature of Ruijie AC product. It is also called ARP Proxy and works as a proxy for a device in the WLAN to respond to the ARP requests of another device. Because CSMA/CA is used for communication in a wireless network, ARP Proxy can prevent ARP broadcast packets in one AP from being sent to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Overview

Feature	Description
Wireless ARP Proxy	AC works as an ARP proxy for wireless STAs to prevent the ARP broadcast requests from being sent to other APs.

15.3.1 Wireless ARP Proxy

Working Principle

In typical wireless networking, a wireless STA usually accesses the Internet through an AP and AC. The typical scenario is that, multiple wireless STAs are associated with one AP while multiple APs are associated with one AC. When wireless STAs under one AP connect to those under another AP, or wireless STAs connect to wired STAs, or wired STAs connect to wireless STAs, ARP packets must be transmitted through AC, facilitating the implementation of AC's ARP Proxy function.

The working process of ARP Proxy is as follows:

24. AC learns the source IP address and source MAC address from the transmitted ARP packet to form an ARP entry.
25. According to the ARP entry, the AC works as a proxy in the network to respond to ARP requests of other users.
26. If the AC does not have the MAC address of the destination host, it forwards the 802.1Q-compliant ARP request.
27. ARP replies are forwarded like 802.1Q-compliant Ethernet frames.

As shown in Figure 15-1, PC3 and PC1 obtain the MAC address of the gateway respectively. Assume that this WLAN has one AC, two APs (AP1 and AP2), and four STAs (PC1, PC2, PC3 and smartphone).

28. PC3 initiates an ARP request to the IP address of the gateway.
29. AP2 forwards this ARP request to PC2 and AC.
30. From this ARP request, AC learns the IP and MAC address of PC3 and forwards this ARP request to the gateway, AP1, and PC1 and the smartphone under AP1.
31. The gateway sends an ARP reply to PC4 through AC. Then AC learns the IP and MAC address of the gateway.
32. PC1 initiates an ARP request to the IP address of the gateway.
33. AP1 forwards this ARP request to PC2 and AC.
34. AC learns the IP and MAC address of PC1 and works as a proxy for the gateway to directly send an ARP reply to PC1. (This is because AC has learned the MAC address of the gateway in step 4. Therefore, ARP request packets will not be broadcast to PC3 and PC4.)

Related Configuration

Enabling Layer-2 ARP Proxy

- By default, Layer-2 ARP Proxy is enabled.
- Run the **no proxy_arp enable** command to disable Layer-2 ARP Proxy.

15.4 Configuration

Configuration	Description and Command	
Enabling Layer-2 ARP Proxy	(Optional) By default, Layer-2 ARP Proxy is enabled.	
	proxy_arp enable	Enables Layer-2 ARP Proxy
Enabling ARP Proxy to learn only ARP packets of wireless ports	(Optional) By default, ARP Proxy learning only ARP packets of wireless ports is disabled.	
	proxy-arp learn only-wlan [**except** *ip_address*]	Enables ARP proxy to learn only ARP packets of wireless ports and excluded IP addresses.

15.4.1 Enabling Layer-2 ARP Proxy

Configuration Effect

Enabling Layer-2 ARP Proxy improves wireless bandwidth efficiency and user experience.

Notes

N/A

Configuration Steps

Enabling Layer-2 ARP Proxy

- By default, Layer-2 ARP Proxy is enabled.
- In a wireless IPv4 scenario, enabling Layer-2 ARP Proxy on AC to better network bandwidth utilization and user experience.

Verification

Run the **show run** command to check whether Layer-2 ARP Proxy is enabled.

Related Commands

Disabling Layer-2 ARP Proxy

Command	**no proxy_arp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Disabling Layer-2 ARP Proxy

Configuration Steps	Disable Layer-2 ARP Proxy.
	`Ruijie(config)# no proxy_arp enable`
Verification	Run the show run command to check if Layer-2 ARP Proxy is enabled.
	`Ruijie# show run` ` no proxy_arp enable`

Common Errors

N/A

15.4.2 Enabling ARP Proxy to Only Learn ARP Packets of Wireless Ports

Configuration Effect

By enabling ARP Proxy to learn only ARP packets of wireless ports, in a simplistic network, ARP entry volume is not used up by ARP packets of wired ports.

Notes

If there is a sufficient ARP Proxy volume, it is not recommended to enable this function, because learning ARP packets of wired ports helps decrease ARP broadcast flooding of wired users.

Configuration Steps

Enabling ARP Proxy to Learn Only ARP Packets of Wireless Ports

- By default, this function is disabled.
- If the AC does not serve as a gateway, when enabling this function, you are recommended to configure an excluded IP address to learn the IP address of the gateway of the wired port.

Verification

Run the **show run** command to check whether this function is enabled.

Related Commands

Enabling ARP Proxy to Learn Only ARP Packets of Wireless Ports

Command	**proxy-arp learn only-wlan** [**except** *ip_address*]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can enable this function when all of the following requirements are met: ● The AC is in centralized forwarding mode. ● The AC is connected with a gateway. SuperVLAN and subVLANs are deployed on the gateway. ● ARP Proxy entries are easily used up due to a large number of users (run the **show proxy-arp statistics** command to display the ARP Proxy statistics).

Configuration Example

Enabling ARP Proxy to Learn Only ARP Packets of Wireless Ports

Configuration Steps	Enable ARP Proxy to learn only ARP packets of wireless ports as well as excluded IP addresses, 192.168.21.1 and 92.168.22.1.
	`Ruijie(config)# proxy-arp learn only-wlan except 192.168.21.1` `Ruijie(config)# proxy-arp learn only-wlan except 192.168.22.1`
Verification	Run the **show run** command to check this function is enabled.

	Ruijie#show run proxy-arp learn only-wlan except 192.168.21.1 proxy-arp learn only-wlan except 192.168.22.1

Common Errors

N/A

15.5 Monitoring

Clearing

Description	Command
Clears the specified ARP Proxy entry.	**clear proxy_arp** *<ip-address vlan-id>*
Clears all ARP Proxy entries.	**clear proxy_arp**

Displaying

Description	Command
Displays all ARP Proxy entries.	**show proxy_arp**
Displays dynamic ARP Proxy entries.	**show proxy_arp dynamic**
Displays the ARP Proxy statistics.	**show proxy_arp statistics**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the receipt/sending status of ARP packets.	**debug proxy_arp**

IP Routing Configuration

1. Configuring Routing Policies
2. Configuring Keys
3. Configuring PBR
4. Configuring RIP
5. Configuring RIPng
6. Configuring OSPFv2
7. Configuring OSPFv3
8. Managing Routes
9. Configuring FPM

1 Configuring Routing Policies

1.1 Overview

Routing policies are a policy set for changing the packet forwarding path or routing information and are often implemented by a filtering list and a route map. Routing policies are flexibly and widely applied in the following methods:

- Use a filtering list in a routing protocol to filter or modify routing information.
- Use a route map in a routing protocol to filter or modify routing information. Where, the route map can further use a filtering list.
- Use a route map in policy-based routing (PBR) to control packet forwarding or modify packet fields.

1.2 Applications

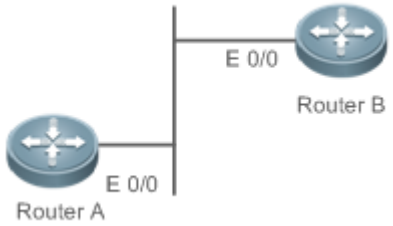
Application	Description
Route Filtering	Use a filtering list in a routing protocol to filter the routing information sent or received by the protocol.
Route Re-distribution	Use a route map in a routing protocol to filter or modify routing information and re-distribute RIP routes to OSPF. Only RIP routes with 4 hops can be re-distributed.
PBR	Use a route map in PBR to control packet forwarding or modify packet fields and specify optimum output interfaces for packets from different subnets.

1.2.1 Route Filtering

By default, a routing protocol advertises and learns all routing information. When a filtering list is used, the routing protocol advertises only required routes or receives only required routing information.

Scenario

Figure 1-1



As shown in Figure 1-1, router A has routes to 3 networks: 10.0.0.0, 20.0.0.0 and 30.0.0.0.
Configure a filtering list on the routers to achieve the following purposes:

- Filter the sent routing information on router A to filter routes that router A does not need to send.

- Filter the received routing information on router B to filter routes that router B does not need to learn.

Deployment

- Filter the sent routing information 30.0.0.0 on router A.
- Filter the received routing information 20.0.0.0 on router B to ensure that router B learns only routing information 10.0.0.0.

1.2.2 Route Re-distribution

By default, route re-distribution will re-distribute all routing information in a routing protocol to another routing protocol. All routing attributes will also be inherited. You can use a route map to perform conditional control for re-distribution between two routing protocols, including:

- Specify the range for re-distributing routes and re-distribute only routing information that meets certain rules.
- Set the attributes of routes generated by re-distribution.

Scenario

Figure 1-2

As shown in Figure 1-2, configure route re-distribution on the devices to achieve the following purposes:

- Re-distribute only RIP routes with 4 hops to OSPF.
- In the OSPF routing domain, the initial metric of this route is 40, the route type is the external route type-1 and the route tag value is set to 40.

Deployment

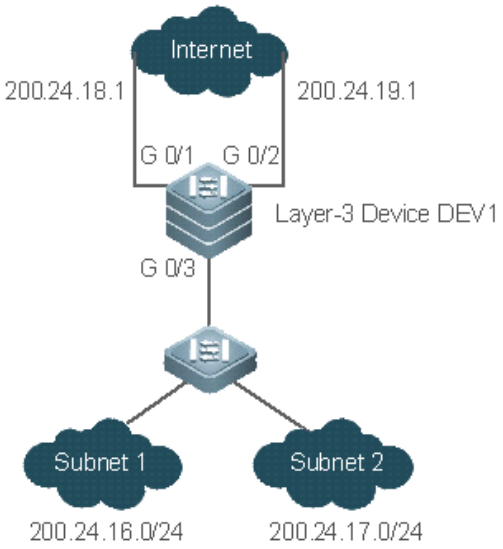
- Configure a route with 4 hops in the route map rip_to_ospf: match, and set the initial metric of this route to 40, the route type to the external route type-1 and the route tag value to 40.
- Configure route re-distribution to re-distribute RIP routes to OSPF and use the route map rip_to_ospf.

1.2.3 PBR

PBR is implemented by applying a route map including policies to interfaces and devices.
Similar to static routing, PBR is also manually configured. It takes effect only in local place and will not update with network changes. As compared with static and dynamic routing, PBR is more flexible. Static and dynamic routing can forward packets only based on destination addresses. PBR can forward packets based on the source and destination addresses, packet length and input interface.

Scenario

Figure 1-3



Configure PBR on the layer-3 device DEV1 to achieve the following purposes:

- Packets from subnet 1 (200.24.16.0/24) are sent from GE0/1 first.
- Packets from subnet 2 (200.24.17.0/24) are sent from GE0/2 first.

Deployment

- Configure two different ACLs to match packets from subnets 1 and 2 respectively.
- Configure the route map RM_FOR_PBR: policy 10 is used to ensure that "packets from subnet 1 are sent from GE0/1 first"; policy 20 is used to ensure that "packets from subnet 2 are sent from GE0/2 first".
- Perform PBR for packets received from GE0/3 and use the route map RM_FOR_PBR.

1.3 Features

Overview

Feature	Description
Filtering List	Define a group of lists based on a route attribute, which can be used by a routing protocol for route filtering.
Route Map	A policy defines "if certain conditions are matched, you can perform certain processing actions".

1.3.1 Filtering List

Filtering lists are a group of lists defined based on a routing attribute and are a tool for filtering routing policies. Independent filtering lists are meaningless and can be used to filter routes only when they are applied in a routing protocol.

Working Principle

Based on different routing attributes, filtering lists are classified into the following types:

Access Control List (ACL)

ACLs comprise IPv4 and IPv6 ACLs. When defining ACLs, you can specify IPv4/IPv6 addresses and masks to match the destination network segment or next-hop addresses of routing information.

For description about ACLs, see the *ACL Configuration Guide*.

Address Prefix List (prefix-list)

Similar to ACLs, prefix-lists, including IPv4 prefix-lists and IPv6 prefix-lists, are used to match destination network segments of routing information during route filtering.

Related Configuration

Creating an ACL

By default, no ACL is configured and no policy is set.

In the global configuration mode, run the **ip access-list** { **extended** | **standard** } { *id* | *name* } command to create an IPv4 ACL.

You can set multiple policies in an ACL, sorted by their sequence numbers. Policies have two working modes: permit and deny.

Creating a Prefix-List

By default, no prefix-list is configured and no entry is set.

In the global configuration mode, run the **ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*] command to create an IPv4 prefix-list and add a prefix entry to the list.

You can set multiple entries in the prefix-list, sorted by their sequence numbers. Entries have two working modes: permit and deny.

Run the **ip prefix-list** *prefix-list-name* **description** *descripton-text* command to add description to the prefix-list.

Run the **ip prefix-list sequence-number** command to enable the sorting function for the prefix-list.

1.3.2 Route Map

A policy is a "match …, set…" statement, which indicates that "if certain conditions are matched, you can perform some processing actions".

Working Principle

Executing policies

A route map may contain multiple policies. Each policy has a corresponding sequence number. A smaller sequence number means a higher priority. Policies are executed based on their sequence numbers. Once the matching condition of a policy is met, the processing action for this policy needs to be performed and the route map exits. If no matching condition of any policy is met, no processing action will be performed.

Working Modes Of Policies

Policies have two working modes:

- permit: When the matching condition of a policy is met, the processing action for this policy will be performed and the route map will exit.
- deny: When the matching condition of a policy is met, the processing action for this policy will not be performed and the route map will exit.

Matching Conditions Of Policies

The matching condition of a policy may contain 0, 1 or more match rules.

- If the matching condition contains 0 match rule, no packet will be matched.
- If the matching condition contains one or more match rules, all rules must be matched.

Processing Action for a Policy

The processing action of a policy may contain 0, 1 or more set rules.

- If the processing action contains 0 set rule, no processing action will be performed and the route map will directly exit.
- If the processing action contains one or more set rules, all processing actions will be performed and then the route map will exit.

⚠ If set rules have different priorities, the set rule with the highest priority will take effect.

Related Configuration

Creating a Route Map (Policy)

By default, no route map is configured and no policy is set.

In the global configuration mode, you can run the **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] command to create a route map and add a policy to the route map.

You can set multiple policies in a route map. Each policy uses different sequence numbers.

Setting Matching Conditions of a Policy

By default, no match rule is set (that is, the matching condition of a policy contains 0 match rule).

In the route map mode, run the **match** command to set match rules. One **match** command is mapped to one match rule.

RGOS provides abundant **match** commands for setting flexible matching conditions.

Command	Description
match interface	Uses the output interface of a route as the matching condition.
match ip address	Uses the destination IPv4 address of a route as the matching condition.
match ip next-hop	Uses the next-hop IPv4 address of a route as the matching condition.
match ip route-source	Uses the source IPv4 address of a route as the matching condition.
match ipv6 address	Uses the destination IPv6 address of a route as the matching condition.
match ipv6 next-hop	Uses the next-hop IPv6 address of a route as the matching condition.
match ipv6 route-source	Uses the source IPv6 address of a route as the matching condition.

Command	Description
match metric	Uses the metric of a route as the matching condition.
match route-type	Uses the type of a route as the matching condition.
match tag	Uses the tag value of a route as the matching condition.

Setting the Processing Actions of a Policy

By default, no set rule is configured (that is, the processing action of a policy contains 0 set rule).

In the route map mode, run the **set** command to configure set rules. One **set** command is mapped to one set rule.

RGOS provides abundant **set** commands for setting flexible processing actions.

Command	Description
set level	Sets the destination area type to which a route will be directed.
set metric	Modifies the metric value of a route.
set metric-type	Sets the metric type of a route.
set next-hop	Sets the next-hop IP address of a route.
set tag	Sets the tag value of a route.

1.4 Configuration

Configuration	Description and Command	
Configuring a Route Map	⚠ (Optional) It is used to define a policy.	
	route-map	Creates a policy (route map).
	match	Sets the matching conditions of the policy.
	set	Sets the processing actions of the policy.
Configuring a Filtering List	⚠ (Optional) It is used to define a filtering list.	
	ip prefix-list	Creates a prefix-list.
	ip prefix-list description	Adds description to a prefix-list.
	ip prefix-list sequence-number	Enables the sorting function for a prefix-list.
	Ipv6 prefix-list	Creates an IPv6 prefix-list.
	ipv6 prefix-list description	Adds description to an IPv6 prefix-list.
	ipv6 prefix-list sequence-number	Enables the sorting function for an IPv6 prefix-list.

1.4.1 Configuring a Route Map

Configuration Effect

- Define a set of routing policies to be used by routing protocols or PBR.

Notes

- If a **match** command uses an ACL to define packet matching conditions, the ACL must be configured.
- The following **match** commands cannot be configured at the same time:

The Following match Commands	Cannot Be Configured with the Following match Commands At the Same Time
match ip address	**match ip prefix-list**
match ipv6 address	**match ipv6 prefix-list**
match ip next-hop	**match ip next-hop prefix-list**
match ipv6 next-hop	**match ipv6 next-hop prefix-list**
match ip route-source	**match ip route-source prefix-list**
match ipv6 route-source	**match ipv6 route-source prefix-list**

Configuration Steps

Creating a Policy (Route Map)

- Mandatory.
- Perform this configuration on a device to which a policy needs to be applied.

Setting Matching Conditions of a Policy

- Optional.
- If no match rule is configured, no packet will be matched.
- If multiple match rules are configured, all the match rules must be matched.
- Perform this configuration on a device to which a policy needs to be applied.

Setting the Processing Actions of a Policy

- Optional.
- If no set rule is configured, no processing action will be performed.
- If multiple set rules are configured, all set rules must be executed (if the set rules have different priorities, the set rule with the highest priority takes effect).
- Perform this configuration on a device to which a policy needs to be applied.

Verification

- Check the configurations of the route map.

Related Commands

Creating a Policy (Route Map)

Command	**route-map** *route-map-name* [{ **permit** | **deny** } *sequence*]
Parameter Description	*route-map-name*: Indicates the name of a route map, comprising not more than 32 characters. permit: Specifies the working mode of this policy as permit, which is the default mode.

	deny: Specifies the working mode of this policy as deny. The default mode is permit. *sequence*: Specifies the sequence number of this policy. A smaller value means a higher priority. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	If this route map is unavailable, this command will create a route map and add a policy to the route map. If this route map is available, this command will add a policy to the route map.

Setting Matching Conditions of a Policy

Command	**match interface** *interface-type interface-number* [*…interface-type interface-number*]
Parameter Description	*interface-type interface-number*: Indicates the interface type and interface number.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the next-hop output interface of a route or a packet.

Command	**match ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the access list number. For a standard access list, the value ranges are 1 to 99 and 1300 to 1999. For an extended access list, the value ranges are 100 to 199 and 2000 to 2699. *access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the destination IPv4 address of a packet or route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured at the same time.

Command	**match ip next-hop** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the access list number. For a standard access list, the value ranges are 1 to 99 and 1300 to 1999. For an extended access list, the value ranges are 100 to 199 and 2000 to 2699. *access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the next-hop IPv4 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured at the same time.

Command	**match ip route-source** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name*

	[*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the access list number. For a standard access list, the value ranges are 1 to 99 and 1300 to 1999. For an extended access list, the value ranges are 100 to 199 and 2000 to 2699. *access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the source IPv4 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured at the same time.

Command	**match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the destination IPv6 address of a packet or route by using an ACL or a prefix-list. An ACL and a prefix list cannot be configured at the same time.

Command	**match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the next-hop IPv6 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured at the same time.

Command	**match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the source IPv6 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured at the same time.

Command	**match length** *min-length max-length*
Parameter Description	*min-length*: Indicates the minimum length of an IP packet. *max-length*: Indicates the maximum length of an IP packet.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the length of an IP packet.

Command	**match metric** *metric*
Parameter Description	*metric*: Indicates the metric value of a route, ranging from 0 to 4,294,967,295.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the metric value of a route.

Command	**match mpls-label**
Parameter Description	-
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match routing information with labels.

Command	**match origin** { **egp** | **igp** | **incomplete** }
Parameter Description	**egp**: Indicates the source is remote EGP. **igp**: Indicates the source is local IGP. **incomplete**: Indicates that the source is an incomplete type.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the source of a route.

Command	**match route-type** {**internal | external** [**type-1 | type-2**] }
Parameter Description	**Internal**: Indicates an internal OSPF route. **external**: Indicates an external route (that of BGP or OSPF). **type-1 | type-2**: Indicates type-1 or type-2 external route of OSPF.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the type of a route.

Command	**match tag** *tag* [*…tag*]
Parameter Description	*tag*: Indicates the tag value of a route.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the tag value of a route.

Setting the Processing Actions of a Policy

Command	**set comm-list** { *community-list-number* | *community-list-name* } **delete**
Parameter Description	*community-list-number*: Indicates the community list number. For a standard community list, the value ranges from 1 to 99. For an extcommunity list, the value ranges from 100 to 199. *community-list-name*: Indicates the community list name, comprising not more than 80 characters.
Command Mode	Route map configuration mode
Usage Guide	This rule is used to delete all community attribute values from the community list for a route matching the match rules.

Command	**set level** {**stub-area** | **backbone** }
Parameter Description	**stub-area**: Indicates that the re-distribution route is advertised to OSPF Stub Area. **backbone**: Indicates that the re-distribution route is advertised to the OSPF backbone area.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the destination area type to which a route will be redirected.

Command	**set metric** [+ *metric-value* | **-** *metric-value* | *metric-value*]
Parameter Description	+: Increases (based on the metric value of the original route). -: Decreases (based on the metric value of the original route). *metric-value*: Sets the metric value of a re-distribution route. A larger value means a lower priority.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to modify the metric value of a route.

Command	**set metric-type** *type*
Parameter Description	*type*: Sets the type of a re-distribution route. The default type of an OSPF re-distribution route is type-2.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the metric type.

Command	**set next-hop** *ip-address*
Parameter Description	*ip-address*: Indicates the next-hop IP address.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the next-hop IP address.

Command	**set tag** *tag*

Parameter Description	*tag*: Sets the tag of a re-distribution route.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the tag value of a route.

Displaying the Configurations of a Route Map

Command	**show route-map** [*name*]
Parameter Description	***name***: Specifies a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Run the **show route-map** command to display the configurations of a route map. If an ACL is used when a route map is configured, you can run the **show access-list** command to display the configurations of the ACL.

Configuration Example

Using a Route Map in Route Re-distribution to Filter and Modify Routing Information

Scenario Figure 1-4	As shown in Figure 1-4, a device is connected to both an OSPF routing domain and RIP routing domain. 
	● Re-distribute only RIP routes with 4 hops to OSPF. In the OSPF route domain, if the route type is the external route type-1, set the tag value of the route to 40. ● Re-distribute only OSPF routes with the tag value 10 to RIP. In the RIP route domain, set the initial metric value of this route to 10.
Configuration Steps	● Configure the route map redrip: Match a route with 4 hours, set the initial metric value of the route to 40, set the route type to the external route type-1, and set the tag value of the route to 40. ● Configure the route map redospf: match a route with the tag value 10 and set the initial metric value of the route to 10. ● Configure re-distribution of the RIP route to OSPF and apply the route map redrip. ● Configure re-distribution of the OSPF route to RIP and apply the route map redospf.
	`Ruijie(config)# route-map redrip permit 10` `Ruijie(config-route-map)# match metric 4` `Ruijie(config-route-map)# set metric-type type-1` `Ruijie(config-route-map)# set tag 40` `Ruijie(config-route-map)# exit` `Ruijie(config)# route-map redospf permit 10`

	Ruijie(config-route-map)# match tag 10 Ruijie(config-route-map)# set metric 10 Ruijie(config-route-map)# exit Ruijie(config)# router ospf 1 Ruijie(config-router)# redistribute rip subnets route-map redrip Ruijie(config-router)# exit Ruijie(config)# router rip Ruijie(config-router)# redistribute ospf 1 route-map redospf Ruijie(config-router)# exit
Verification	● Check the configurations of the route map to verify the policy rules. ● Check the OSPF routing information library to verify that the rules matching the policy rules are re-distributed.
	Ruijie# show route-map route-map redrip, permit, sequence 10 Match clauses: metric 4 Set clauses: metric 40 metric-type type-1 tag 40 route-map redospf, permit, sequence 10 Match clauses: tag 10 Set clauses: metric 10
	Ruijie# show ip ospf database external OSPF Router with ID (192.100.1.9) (Process ID 1) AS External Link States

```
LS age: 5
Options: 0x2 (-|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 192.168.199.0 (External Network Number)
Advertising Router: 192.100.1.9
LS Seq Number: 80000001
Checksum: 0x554d
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
      Metric: 4
      Forward Address: 0.0.0.0
      External Route Tag: 40
```

Common Errors

- After matching of ACLs and prefix-lists is configured, the corresponding ACLs and prefix lists are not defined.

1.4.2 Configuring a Filtering List

Configuration Effect

- Define a set of route filtering rules to be used by routing protocols.

Notes

- A configured filtering list can take effect only after it is associated with a routing protocol.

Configuration Steps

Configuring a Prefix-List

- To filter address prefixes, you should perform this configuration.
- If there is no special requirement, you should perform this configuration on a route for which filtering based on a prefix-list needs to be performed.

Configuring an AS Path List

- To filter address prefixes, you should perform this configuration.
- If there is no special requirement, you should perform this configuration on a route for which filtering based on an AS path needs to be performed.

Configuring a Community List

- To filter community attributes, you should perform this configuration.
- If there is no special requirement, you should perform this configuration on a route for which community attributes need to be filtered.

Configuring an Extcommunity List

- To filter extended community attributes, you should perform this configuration.
- If there is no special requirement, you should perform this configuration on a route for which extended community attributes need to be filtered.

Verification

- Check whether the filtering list is correctly configured.
- Check the routing table to verify that routes can be correctly filtered.

Related Commands

Creating a Prefix-List

Command	**ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *seq-number*: Assigns a sequence number to an prefix-list entry, ranging from 1 to 2,147,483,647. If this command does not contain the sequence number, the system will assign a default sequence number to the prefix-list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each entry not assigned with a value is the first multiple of 5 greater than the previous sequence number. **deny:** Denies access when certain conditions are matched. **permit:** Permits access when certain conditions are matched. ***ip-prefix*:** Configures the IP address and mask, ranging from 0 to 32 digits. ***minimum-prefix-length*:** Specifies the minimum range (namely, the start length of a range). ***maximum-prefix-length*:** Specifies the maximum range (namely, the end length of a range).
Command Mode	Global configuration mode
Usage Guide	-

Adding Description to a Prefix-List

Command	**ip prefix-list** *prefix-list-name* **description** *descripton-text*
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *descripton-text*: Describes the prefix-list.
Command Mode	Global configuration mode

Usage Guide	-

Enabling the Sorting Function for a Prefix-List

Command	**ip prefix-list sequence-number**
Parameter Description	**-**
Command Mode	Global configuration mode
Usage Guide	-

Creating an IPv6 Prefix-List

Command	**ipv6 prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Parameter Description	***prefix-list-name*:** Indicates the prefix-list name. ***seq-number*:** Assigns a sequence number to an prefix-list entry, ranging from 1 to 2,147,483,647. If this command does not contain the sequence number, the system will assign a default sequence number to the prefix-list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each entry not assigned with a value is the first multiple of 5 greater than the previous sequence number. **deny:** Denies access when certain conditions are matched. **permit:** Permits access when certain conditions are matched. ***ipv6-prefix*:** Configures the IP address and mask, ranging from 0 to 128 digits. ***minimum-prefix-length*:** Specifies the minimum range (namely, the start length of a range). ***maximum-prefix-length*:** Specifies the maximum range (namely, the end length of a range).
Command Mode	Global configuration mode
Usage Guide	-

Adding Description to an IPv6 Prefix List

Command	**ipv6 prefix-list** *prefix-list-name* **description** *descripton-text*
Parameter Description	***prefix-list-name***: Indicates the prefix list name. *descripton-text*: Describes the prefix list.
Command Mode	Global configuration mode
Usage Guide	-

Enabling the Sorting Function for an IPv6 Prefix-List

Command	**ipv6 prefix-list sequence-number**
Parameter Description	**-**
Command	Global configuration mode

Mode	
Usage Guide	-

Common Errors

- A filtering list is configured but is not correctly applied in a routing protocol, which causes that the filtering list cannot take effect.

1.5 Monitoring

Displaying

Description	Command
Displays the configurations of a route map.	**show route-map** [*route-map-name*]
Displays the configurations of an ACL.	**show access-lists** [*id* | *name*]
Displays the configurations of an IPv4 prefix-list.	**show ip prefix-list** [*prefix-name*]
Displays the configurations of an IPv6 prefix-list.	**show ipv6 prefix-list** [*prefix-name*]

2 Configuring Keys

2.1 Overview

Keys are a kind of parameters that are used in algorithms for conversion from plain text to cipher text or from cipher text to plain text.

Plain text and cipher text authentication are supported for packet authentication in a routing protocol, during which keys need to be used.

At present, keys are used only for RIP packet authentication.

2.2 Applications

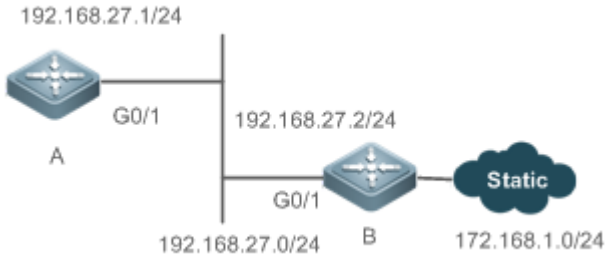
Application	Description
RIP Authentication	RIP uses keys for packet authentication.

2.2.1 RIP Authentication

Scenario

Network devices run RIP and use the MD5 authentication mode to increase the protocol security.

Figure 2-1



Deployment

- Configure a key chain on A. Configure RIP to enable packet authentication and use the key chain.
- Configure a key chain on B. Configure RIP to enable packet authentication and use the key chain.

2.3 Features

Overview

Feature	Description
Key Chain	Provide a tool for authentication in a routing protocol.

2.3.1 Key Chain

Working Principle

A key chain may contain multiple different keys. Each key contains the following attributes:

- Key ID: Identifies a key. In the current key chain, keys and IDs are mapped in the one-to-one manner.
- Authentication string: Indicates a set of key characters used for verifying the consistency of authentication strings in a routing protocol.
- Lifetime: Specifies the lifetime of the current key for sending or receiving packets. Different authentication keys can be used in different periods.

Related Configuration

Creating a Key Chain and a Key

In the global configuration mode, run the **key chain** *key-chain-name* command to define a key chain and enter the key chain configuration mode.

In the key chain configuration mode, run the **key** *key-id* command to define a key and enter the key chain key configuration mode.

Configuring an Authentication String

In the key chain key configuration mode, run the **key-string** [**0**|**7**] *text* command to specify an authentication string.

- A plain text authentication string is configured by default. The value **0** indicates that a plain text authentication key is configured.
- The value **7** indicates that a cipher text authentication string is configured.
- The encryption authentication service is disabled by default. You can run the **service password-encryption** command to enable the encryption service to forcibly convert plain text authentication into cipher text.

Configuring Lifetime

In the key chain key configuration mode, you can configure the lifetime of a key chain in the receiving and sending directions.

- **accept-lifetime** *start-time* { **infinite |** *end-time* **| duration** *seconds* }: Configures the lifetime of a key chain in the receiving direction.
- **send-lifetime** *start-time* { **infinite |** *end-time* **| duration** *seconds* }: Configures the lifetime of a key chain in the sending direction.

2.4 Configuration

Configuration	Description and Command

Configuring a Key Chain	(Mandatory) It is used to create a key.	
	key chain	Creates a key chain.
	key	Configures a key ID.
	key-string	Configures a key string.
	accept-lifetime	Configures the lifetime in the receiving direction.
	send-lifetime	Configures the lifetime in the sending direction.

2.4.1 Configuring a Key Chain

Configuration Effect

- Define a key chain to be used by a routing protocol.

Notes

- A key chain can take effect only after it is associated with a routing protocol.

Configuration Steps

Creating a Key Chain

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configuring a Key ID

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configuring a Key String

- This configuration is mandatory if a key chain needs to be used.
- If there is no special requirement, you should perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configure the Lifetime in the Receiving Direction

- Optional.
- If the lifetime in the sending direction is not configured, the key chain will be always effective.

Configure the Lifetime in the Sending Direction

- Optional.

- If the lifetime in the sending direction is not configured, the key chain will be always effective.

Verification

- Use keys in a routing protocol and observe the neighborship established by the routing protocol. If the keys are inconsistent, the neighborship fails to be established.

Related Commands

Configuring a Key Chain

Command	**key chain** *key-chain-name*
Parameter Description	*key-chain-name*: Indicates the name of a key chain.
Command Mode	Global configuration mode
Usage Guide	To make a key chain take effect, you must configure at least one key.

Configuring a Key ID

Command	**key** *key-id*
Parameter Description	*key-id*: Indicates the authentication key ID in a key chain, ranging from 0 to 2,147,483,647.
Command Mode	Key chain configuration mode.
Usage Guide	-

Configuring a Key Authentication String

Command	**key-string** [**0**|**7**] *text*
Parameter Description	**0:** Specifies that the key is displayed in plain text. **7:** Specifies that the key is displayed in cipher text. ***text*:** Specifies the authentication string characters.
Command Mode	Key chain key configuration mode.
Usage Guide	-

Configuring the Lifetime in the Sending Direction

Command	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
Parameter Description	***start-time*:** Indicates the start time of the lifetime. **infinite:** Indicates that the key is always effective. ***end-time*:** Indicates the end time of the lifetime, which must be later than start-time. **duration *seconds*:** Specifies the duration from the start time to the end time, ranging from 1 to 2,147,483,646.
Command	Key chain key configuration mode.

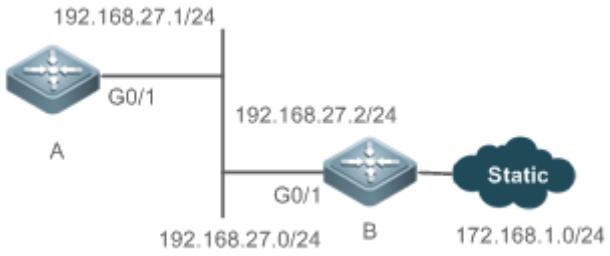
Mode	
Usage Guide	Run this command to define the lifetime of the key in the sending direction.

Configuring the Lifetime in the Receiving Direction

Command	**accept-lifetime** *start-time* **{infinite |** *end-time* **| duration** *seconds***}**
Parameter Description	***start-time*:** Indicates the start time of the lifetime. **infinite:** Indicates that the key is always effective. ***end-time*:** Indicates the end time of the lifetime, which must be later than start-time. **duration *seconds*:** Specifies the duration from the start time to the end time, ranging from 1 to 2,147,483,646.
Command Mode	Key chain key configuration mode.
Usage Guide	Run this command to define the lifetime of the key in the receiving direction.

Configuration Example

Configuring a Key Chain and Using the Key Chain in RIP Packet Authentication

Scenario Figure 2-2	
Configuration Steps	● Configure a key on all routers. ● Configure RIP on all routers. ● Enable RIP authentication on all routers.
A	`A>enable` `A#configure terminal` `A(config)#key chain ripchain` `A(config-keychain)#key 1` `A(config-keychain-key)#key-string Hello` `A(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200` `A(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200` `A(config-keychain-key)#exit` `A(config-keychain)#key 2`

	A(config-keychain-key)#key-string World A(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#exit A(config)#interface gigabitEthernet 0/1 A(config-if)#ip address 192.168.27.1 255.255.255.0 A(config-if)#ip rip authentication key-chain ripchain A(config-if)#ip rip authentication mode md5 A(config-if)#exit A(config)#router rip A(config-router)#version 2 A(config-router)#network 192.168.27.0
B	B>enable B#configure terminal B(config)#key chain ripchain B(config-keychain)#key 1 B(config-keychain-key)#key-string Hello B(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#exit B(config-keychain)#key 2 B(config-keychain-key)#key-string World B(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#exit B(config)#interface gigabitEthernet 0/1 B(config-if)#ip address 192.168.27.2 255.255.255.0 B(config-if)#ip rip authentication key-chain ripchain B(config-if)#ip rip authentication mode md5 B(config-if)#exit B(config)#router rip

	B(config-router)#version 2 B(config-router)#network 192.168.27.0 B(config-router)#redistribute static
Verification	Run the **show ip route rip** command to check whether router A can receive an RIP route from router B.
A	A(config)#show ip route rip R 172.168.0.0/16 [120/1] via 192.168.27.2, 00:05:16, GigabitEthernet 0/1

Common Errors

- A key is not correctly associated with a routing protocol, which causes that authentication does not take effect.
- The keys configured on multiple routers are not consistent, which causes authentication failure.

2.5 Monitoring

Displaying

Description	Command
Displays the configurations of a key chain.	**show key chain** [*key-chain-name*]

3 Configuring PBR

3.1 Overview

Policy-based routing (PBR) is implemented by applying a route map including policies to interfaces and devices.

Similar to static routing, PBR is also manually configured and cannot automatically update with network changes. In addition, PBR is effective only for packets sent from local interfaces and devices. As compared with static and dynamic routing, PBR is more flexible. Static and dynamic routing can forward packets only based on destination addresses. PBR can forward packets based on destination addresses and input interface.

3.2 Applications

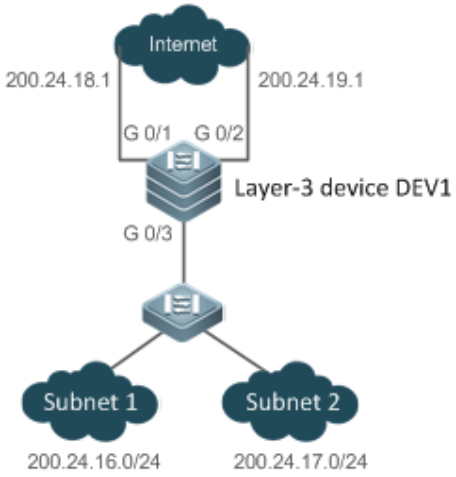
Application	Description
Selecting an ISP by Using PBR	Specify preferential output interfaces for packets from different subnets.

3.2.1 Selecting an ISP by Using PBR

An existing user network often uses resources of multiple internet server providers (ISPs). PBR needs to be used since different bandwidths may be requested from different ISPs or the network resources for key users need to be protected. By controlling forwarding of certain data packets, you can make full use ISP resources as well as meet the requirements of flexible and diversified applications.

Scenario

Figure 3-1



A LAN has two output interfaces for connecting the Internet. PBR is configured on the layer-3 device DEV1 to enable the two output interfaces to implement load sharing and mutual backup.

The specific requirements are as follows:

- Data streams from subnet 1 are sent from GE 0/1.
- Data streams from subnet 2 are sent from GE 0/2.
- If the GE 0/1 link is disconnected, the data streams on GE 0/1 are switched to GE 0/2. Vice versa.

Deployment

- Configure two different ACLs on the layer-3 device DEV1:
  ACL1: source addresses belong to subnet 1.
  ACL2: source addresses belong to subnet 2.
- Configure two policies in the route map on the layer-3 device DEV1:
  Policy 1: sets the next hops for packets matching ACL1 to GE0/1 and GE0/2 (Based on the configuration sequence, GE0/1 takes effect first and GE0/2 works in the backup mode).
  Policy 2: sets the next hops for packets matching ACL2 to GE0/2 and GE0/1 (Based on the configuration sequence, GE0/2 takes effect first and GE0/1 works in the backup mode).
- Configure PBR on GE0/3 (by using a route map). Then, packets received on this interface are forwarded based on the policies.

3.3 Features

Feature	Description
Configuring a Policy	Before configuring PBR, configure policies in a route map.
Configuring PBR	Apply a route map including policies to interfaces and devices to implement PBR.

3.3.1 Configuring a Policy

A policy is a "match …, set…" statement, which indicates that "if certain conditions are matched, perform certain processing actions".

For detailed introduction to the policies, see the section "Route Map".

Executing Policies

In the global configuration mode, you can run the **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] command to create a policy in a route map.

A route map may contain multiple policies. Each policy has a corresponding sequence number. A smaller sequence number means a higher priority. Policies are executed based on their sequence numbers. Once the matching condition of a policy is met, the processing action for this policy needs to be executed and the route map exits. If no matching condition of any policy is met, no processing action will be performed.

Policies have two working modes:

- permit: When the matching condition of a policy is met, perform the processing action for this policy and exit the route map.
- deny: When the matching condition of a policy is met, do not perform the processing action for this policy and exit the route map.

Matching conditions of policies

The matching conditions of a policy may contain 0, 1 or more matching rules.

- If 0 matching rule is contained, no packet will be matched.
- If one or more match rules are contained, all match rules must be matched at the same time to meet the matching conditions of the policy.

In the route map mode, run the **match** command to configure match rules. One **match** command is mapped to one match rule.

PBR supports the following **match** commands:

	Command	Description
IPv4 PBR	**match ip address**	The source IPv4 address (and the destination IPv4 address) is used as the matching condition. Multiple **match ip address** commands can be configured in a policy.
IPv6 PBR	**match ipv6 address**	The source IPv6 address (and the destination IPv6 address) is used as the matching condition. Only one **match ipv6 policy** command can be configured in a policy.

IPv4 PBR defines the source IP address (and destination IP address) ranges of packets by using the IP standard or extended ACLs. IPv6 PBR defines the source IPv6 address (and destination IPv6 address) ranges of packets by using the IPv6 extended ACLs.

Packet forwarding based on policies of IPv4 PBR interfaces supports expert-level and MAC name ACLs. Packet forwarding based on local policies does not support expert-level and MAC name ACLs.

When PBR uses an ACL that is unavailable, the route sub-map will not be matched and the next route sub-map will be matched instead. If no route sub-map is matched, a common route will be selected for forwarding. If only ACLs are configured but no ACE is configured, the PBR forwarding behavior is the same as that in a scenario where an ACL is unavailable.

Processing action for a policy

The processing action of a policy may contain 0, 1 or more set rules.

- If 0 set rule is contained, no processing action will be performed and the route map will directly exit.

- If one or more set rules are contained, all processing actions will be performed and the route map will exit.

If set rules have different priorities, the set rule with the highest priority will take effect.

In the route map mode, run the **set** command to configure set rules. One **set** command is mapped to one set rule.

PBR supports the following **set** commands:

	Command	Description
IPv4 PBR	**set vrf**	Sends IPv4 packets to a VRF for forwarding. Select routes for packets matching the match rules by using a VRF specified by **set vrf**, no matter whether the interface that receives the packets belongs to the VRF. This command cannot work with the **set interface** and **set default interface** commands.
	set ip next-hop	Configures the next hop of IPv4 packet forwarding. The next hop must be directly connected; otherwise, this command is invalid. A packet matching the match rules will be forwarded to the next hop specified by **set ip next-hop first**, no matter whether the route selected for the packet in the routing table is consistent with the next hop specified by PBR. On a switch, the output interfaces for next hops supported by PBR include the SVI, routing and layer-3 AP interfaces.
	set interface	Configures the output interface of IPv4 packet forwarding. A packet matching the match rules will be forwarded from the interface specified by **set interface** first, no matter whether the route selected for the packet in the routing table is consistent with the output interface specified by PBR. This command cannot work with the **set vrf** command.
	set ip default next-hop	Configures the default next hop of IPv4 packet forwarding. A packet matching the match rules will be forwarded to the default next hop specified by this command if a route fails to be selected or the default route is selected for this packet in the routing table.
	set ip default interface	Configures the default output interface of IPv4 packet forwarding. A packet matching the match rules will be forwarded from the interface specified by this command if a route fails to be selected or the default route is selected for this packet in the routing table. This command cannot work with the **set vrf** command.

	Command	Description
IPv6 PBR	**set ipv6 next-hop**	Configures the next hop of IPv6 packet forwarding. An IPv6 packet matching the match rules will be forwarded to the next hop specified by **set ipv6 next-hop** first, no matter whether the route selected for the IPv6 packet in the routing table is consistent with the next hop specified by PBR. The next hop must be directly connected; otherwise, this command is invalid.
	set ipv6 default next-hop	Configures the default next hop of IPv6 packet forwarding. An IPv6 packet matching the match rules will be forwarded to the default next hop specified by this command if a route fails to be selected or the default route is selected for this packet in the routing table. The next hop must be directly connected; otherwise, this command is invalid.

The priority sequence is as follows: **set ip next-hop > set ip next-hop recursive > set interface >** common route **> set ip default next-hop > set default interface >** default route. The preceding **set** commands can be configured at the same time but only the command with the highest priority takes effect.

The priority sequence is as follows: **set ipv6 next-hop >** common route **> set ipv6 default next-hop >** default route**.** The preceding **set** commands can be configured at the same time but only the command with the highest priority takes effect.

3.3.2 Configuring PBR

PBR

Apply a route map including policies to interfaces or devices to implement PBR.

- Apply a route map to an interface so that packets received by the interface are routed based on the policy.
  The PBR is often used to control user packets received by a device. This command is effective only for forwarded packets, but not for locally initiated packets.
- Apply a route map to a device so that packets locally initiated are routed based on the policy.
  The PBR is often used to control protocol packets exchanged between devices (such as ping packets sent locally). This command is effective only for locally initiated packets, but not for forwarded packets.

By default, PBR is not unavailable on a device and packets are forwarded based on a routing table.

Redundant backup or load balancing

You can set multiple next hops in a policy. Either redundant backup or load balancing can be implemented among multiple next hops. Redundant backup is implemented by default.

Redundant backup or load balancing is only effective for next hops configured in the **set ip next-hop**, **set ip next-hop recursive**, **set ip default next-hop**, **set ipv6 next-hop** and **set ipv6 default next-hop** commands, and only effective among multiple next hops in the same set rule.

- Redundant backup
  Based on the configuration sequence, the first accessible next hop takes effect. When the currently effective next hop (R1) is faulty, the traffic automatically switches to the next accessible next hop (R2). When R1 becomes accessible again, the traffic automatically switches back to R1.
  A newly added next hop is arranged at the last of the sequence. Assume that the original sequence of multiple next hops is R1 > R2 > R3. After R1 is deleted and added again, the sequence changes to R2 > R3 > R1.
  If no next hop is accessible, packets will be discarded.
- Load balancing
  When multiple accessible next hops take effect at the same time, the Weighted Cost Multiple Path (WCMP) and Equal Cost Multiple Path (ECMP) are supported. After an accessible next hop loses effect, traffic will be balanced among the other accessible next hops.

Correlation with BFD

Correlation between PBR and BFD is effective only for next hops configured by the **set ip next-hop** or **set ipv6 next-hop** command.

The **set ip next-hop** and **set ipv6 next-hop** commands carry the **verify-availability** and **bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* parameters, which can establish correlation between PBR and a BFD session and monitor the accessibility of next hops.

Correlation between PBR and BFD helps enhance the PBR's perception about network environment changes. When BFD detects that the current next hop is not accessible, the BFD will immediately notify the PBR to switch the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

For the configuration and related commands for correlation between PBR and BFD, see the "BFD" section.

Correlation with Track

Correlation between PBR and Track is effective only for next hops configured by the **set ip next-hop** command.

The **set ip next-hop** command carries the **verify-availability** and **track** *track-obj-number* parameters, which can establish correlation between PBR and a Track session and monitor the accessibility of next hops.

Correlation between PBR and Track helps enhance the PBR's perception about network environment changes. When Track detects that the current next hop is not accessible, the Track will immediately notify the PBR to switch the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

Only IPv4 PBR supports correlation with Track.

For the configuration and related commands for correlation between PBR and Track, see the "RNS" section.

VRF transfer

If this feature is selected for VRF based on PBR, an interface to which PBR is applied can filter received IP packets by using the match rules. If the packets are successfully matched, the interface will specify a VRF instance for route selection in the set rules. The match rules include ACL (IP access list). Since the match rules are flexible, you can allocate different traffic to different VRF instances based on actual requirements.

Generally, packets received on a VRF interface will be forwarded from this VRF interface, and packets received on a global interface will be forwarded based on a global routing table. PBR can break this limit and enable packets to be transferred between VRF and a global route map. The specific information is as follows:

- From a global routing table to VRF: Packets received from a global interface are transferred to a specified VRF instance for forwarding.
- From a VRF instance to another VRF: instance: Packets received from a VRF interface are transferred to another VRF interface for forwarding.
- From VRF to a global routing table: Packets received from a VRF interface are transferred to the global routing table for forwarding.

Single-protocol VRF enables packets to be transferred only to VRF instances using IPv4 PBR. Multi-protocol VRF enables packets to be transferred to VRF instances using IPv4 and IPv6 PBR.

For VRF configuration and related commands, see the "VRF" section.

Only the following **set** commands enable packets to be transferred between VRFs or global routing tables.

Command	Description
set vrf	Transfers packets from a global routing table to a VRF instance, and then from the VRF instance to another VRF instance.
set ip next-hop	Carries the **vrf** *vrf-name* and **global** parameters. Configures **vrf** *vrf-name* to transfer packets from a global routing table to a VRF instance and from the VRF instance to another VRF instance. Configures **global** to transfer packets from a VRF instance to a global routing table.
set ipv6 next-hop	Carries the **vrf** *vrf-name* and **global** parameters. Configures **vrf** *vrf-name* to transfer packets from a global routing table to a VRF instance and from the VRF instance to another VRF instance. Configures **global** to transfer packets from a VRF instance to a global routing table.

3.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of PBR	(Mandatory) It is used to apply PBR to forward packets.	
	ip policy route-map	Applies PBR for IPv4 packets received by an interface.
	ipv6 policy route-map	Applies PBR for IPv6 packets received by an interface.

Configuration	Description and Command	
	ip local policy route-map	Applies PBR for IPv4 packets locally initiated.
	ipv6 local policy route-map	Applies PBR for IPv6 packets locally initiated.
Setting Redundant Backup or Load Balancing	(Optional) It is used to set whether PBR implements redundant backup or load balancing among multiple next hops.	
	ip policy { **redundance** | **load-balance** }	Sets whether IPv4 PBR implements redundant backup or load balancing among multiple next hops. The default setting is redundant backup.
	ipv6 policy { **redundance** | **load-balance** }	Sets whether IPv6 PBR implements redundant backup or load balancing among multiple next hops. The default setting is redundant backup.

3.4.1 Configuring Basic Functions of PBR

Configuration Effect

Perform personalized routing management for user data streams by preparing flexible policies.

Perform personalized management for protocol interaction and network topologies by preparing flexible policies.

Notes

- A route map must be used when PBR is configured; therefore, you must configure a route map on a device.
- If an ACL is used when the route map is configured, you must configure the ACL on the device.

Configuration Steps

↘ Applying PBR for IPv4 packets received by an interface

- To perform personalized routing management for IPv4 user data streams passing a device, you should perform this configuration.
- Perform this configuration on the input interface for user data streams.
- Run the **ip policy route-map** command to apply a route map to an interface. Then, PBR is executed for IPv4 packets received on this interface.

Command	**ip policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command	Interface configuration mode

Mode	
Usage Guide	Only one **ip policy route-map** command can be configured for an interface. If multiple **ip policy route-map** commands are configured for an interface, only the last configuration takes effect. If the route map used in PBR is unavailable, the PBR does not take effect.

Applying PBR for IPv6 packets received by an interface

- To perform personalized routing management for IPv6 user data streams passing a device, you should perform this configuration.
- Perform this configuration on the input interface for user data streams.
- Run the **ipv6 policy route-map** command to apply a route map to an interface. Then, PBR is executed for IPv6 packets received on this interface.

Command	**ipv6 policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command Mode	Interface configuration mode
Usage Guide	Only one **ipv6 policy route-map** command can be configured for an interface. If multiple **ipv6 policy route-map** commands are configured for an interface, only the last configuration takes effect. If the route map used in PBR is unavailable, the PBR does not take effect.

Applying PBR for IPv4 packets locally initiated

- To perform personalized management for IPv4 protocol interaction and IPv4 network topologies, you should perform this configuration.
- Run the **ip local policy route-map** command to apply a route map to a device. Then, PBR is executed for IPv4 packets locally initiated.

Command	**ip local policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command Mode	Global configuration mode
Usage Guide	Only one **ip local policy route-map** command can be configured for a device. If the route map used in PBR is unavailable, the PBR does not take effect.

Applying PBR for IPv6 packets locally initiated

- To perform personalized management for IPv6 protocol interaction and IPv6 network topologies, you should perform this configuration.

- Run the **ipv6 local policy route-map** command to apply a route map to a device. Then, PBR is executed for IPv6 packets locally initiated.

Command	**ipv6 local policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is unavailable on a device and packets are forwarded based on a routing table.
Command Mode	Global configuration mode
Usage Guide	Only one **ipv6 local policy route-map** command can be configured for a device. If the route map used in PBR is unavailable, the PBR does not take effect.

Verification

- Check the configurations of PBR.
- Check the configurations of the route map used by PBR.
- If an ACL is used when the route map is configured, you should check the configurations of the ACL.

Checking the configurations of IPv4 PBR

Command	**show ip policy** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Check the interfaces configured with IPv4 PBR according to the output information and the name of the used route map. `Ruijie# show ip policy` `Banlance mode: redundance` `Interface Route map` `local RM_for_PBR_1` `GigabitEthernet 0/1 RM_for_PBR_2` **Local** indicates applying policy-based routing for IPv4 packets locally initiated.

Checking the configurations of IPv6 PBR

Command	**show ipv6 policy** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Check the interfaces configured with IPv6 PBR according to the output information and the name of the used

	route map. `Ruijie#show ipv6 policy` `Banlance mode: redundance` `Interface Route map` `local RM_for_PBR_1` `VLAN 1 RM_for_PBR_2` **Local** indicates applying policy-based routing for IPv6 packets locally initiated.

Checking the configurations of a route map

Command	**show route-map** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Multiple route maps may be available on a device. Focus on the route map used in PBR and check its policy settings. `Ruijie# show route-map` `route-map RM_FOR_PBR, permit, sequence 10` `Match clauses:` `ip address acl1` `Set clauses:` `ip next-hop 200.24.18.1` `route-map RM_FOR_PBR, permit, sequence 20` `Match clauses:` `ip address acl2` `Set clauses:` `ip next-hop 200.24.19.1`

Checking the configurations of an ACL

Command	**show access-lists** [*acl-id* | *acl-name*]
Parameter Description	*acl-id*: Indicates the ACL ID. *acl-name*: Indicates the ACL name.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Multiple ACLs may be available on a device. Focus on the ACL used by a route map and check its configurations.

```
Ruijie# show access-lists 1
ip access-list standard 1
 10 permit 200.24.16.0 0.0.0.255
ip access-list standard 2
 10 permit 200.24.17.0 0.0.0.255
```

Checking the routing information of IPv4 PBR

Command	**show ip pbr route** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a local interface or device and check the routing information of IPv4 PBR.

```
Ruijie# show ip pbr route
PBR IPv4 Route Summay : 1
Interface        : GigabitEthernet 0/1
  Sequence       : 10
  VRF ID         : 0
  Route Flags    :
   Route Type    : PBR
   Direct        : Permit
   Priority      : High
   Precedence    : None
  Precedence     : 0
  Mode           : redundance
  Nexthop Count  : 1
   Nexthop[0]    : 192.168.8.100
   Weight[0]     : 1
   Ifindex[0]    : 2
```

Checking the routing information of IPv6 PBR

Command	**show ipv6 pbr route** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.

Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a local interface or device and check the routing information of IPv6 PBR. `Ruijie# show ipv6 pbr route` `PBR IPv6 Route Summary : 1` `Interface : GigabitEthernet 0/1` `Sequence : 10` `ACL[0] : 2900` `ACL_CLS[0] : 5` `VRF ID : 0` `Route Flags :` `Route Type : PBR` `Direct : Permit` `Priority : High` `Precedence : None` `Precedence : 0` `Mode : redundance` `Nexthop Count : 1` `Nexthop[0] : 10::2` `Weight[0] : 1` `Ifindex[0] : 2`

Checking a route map used by IPv4 PBR

Command	**show ip pbr route-map** *rmap-name*
Parameter Description	*rmap-name*: Indicates the route map name.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a route map and check the route map used by IPv4 PBR. `Ruijie# show ip pbr route-map rm` `PBR VRF: GLOBAL, ID: 0` `Forward Mode: redundance` `Forwarding: On`

	Route-map rm Route-map index: Sequence 10, permit Match rule: ACL ID : 2900, CLS: 1, Name: acl1 Set rule: IPv4 nexthop: 192.168.8.100, (VRF name: , ID: 0), Weight: 0 PBR state info ifx: 2, Connected: True, Track state: Up

Checking a route map used by IPv6 PBR

Command	**show ipv6 pbr route-map** *rmap-name*
Parameter Description	*rmap-name*: Indicates the route map name.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	Specify a route map and check the route map used by IPv6 PBR. Ruijie# show ipv6 pbr route-map rm6 PBR VRF: GLOBAL, ID: 0 Forward Mode: redundance Forwarding: On Route-map rm6 Route-map index: Sequence 10, permit Match rule: ACL ID : 2901, CLS: 5, Name: acl6 Set rule: IPv6 nexthop: 10::2, (VRF name: , ID: 0), Weight: 0 PBR state info ifx: 2, Connected: True, Track state: Up

Checking the statistics about packets forwarded by IPv4 PBR

Command	**show ip pbr statistics** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.
Command Mode	Privilege, global and interface configuration modes

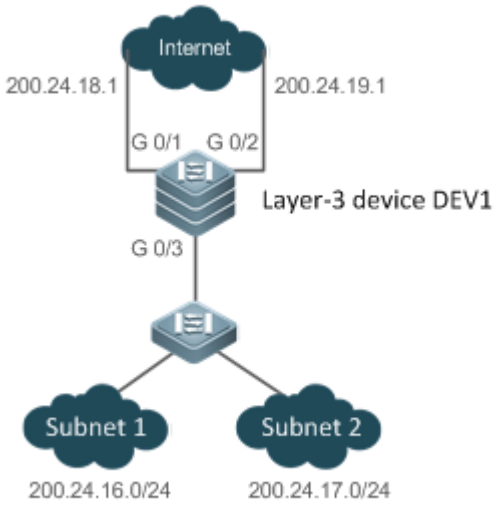
Usage Guide	`Ruijie# show ip pbr statistics` `IPv4 Policy-based route statistic` `gigabitEthernet 0/1` `  statistics : 10`

Checking the statistics about packets forwarded by IPv6 PBR

Command	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates local.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	`Ruijie# show ipv6 pbr statistics` `IPv6 Policy-based route statistic` `gigabitEthernet 0/1` `  statistics : 20`

Configuration Example

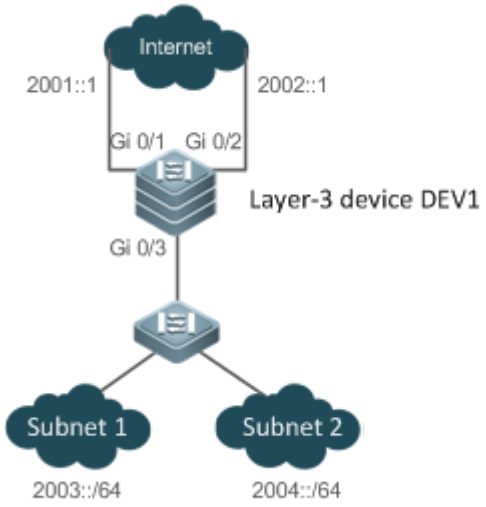
Configuring IPv4 PBR and selecting an output link based on source addresses of packets

Scenario **Figure 3-2**	
	The layer-3 device DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24 whereas the network segment where subnet 2 resides is 200.24.17.0/24. DEV 1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.

	This LAN has two output interfaces for connecting the Internet. The requirements are as follows: ● Data streams from subnet 1 for accessing the Internet should pass GE 0/1. ● Data streams from subnet 2 for accessing the Internet should pass GE 0/2. ● If the GE 0/1 link is disconnected, the data streams on the GE 0/1 interface are switched to the GE 0/2 interface. Vice versa.
Configuration Steps	● Configure two ACLs to match packets from subnets 1 and 2 respectively. ● Set a policy to set the next hops for packets from subnet 1 to GE0/1 and GE0/2. (Pay attention to the configuration sequence.) ● Set a policy to set the next hops for packets from subnet 2 to GE0/2 and GE0/1. (Pay attention to the configuration sequence.) ● Apply the policy to GE 0/3. ● Set PBR to implement redundant backup among multiple next hops. (The default setting is redundant backup.) During redundant backup, based on the configuration sequence, the first next hop takes effect first.
	DEV1(config)# access-list 1 permit 200.24.16.0 0.0.0.255 DEV1(config)# access-list 2 permit 200.24.17.0 0.0.0.255 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 2 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Verification	● Check the configurations of IPv4 PBR.

	• Check the configurations of the route map. • Check the configurations of an ACL.
	DEV1# show ip policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address 1 Set clauses: ip next-hop 200.24.18.1 200.24.19.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address 2 Set clauses: ip next-hop 200.24.19.1 200.24.18.1
	DEV1# show access-lists ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255 ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

Configuring IPv6 PBR and selecting an output link based on source addresses of packets

Scenario **Figure 3-3**	
	DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 2003::/64 whereas the network segment where subnet 2 resides is 2004::/64. DEV1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 2001::1/64 and 2002::1/64.
	This LAN has two output interfaces for connecting the Internet. The requirements are as follows: ● Data streams from subnet 1 for accessing the Internet should pass GE 0/1. ● Data streams from subnet 2 for accessing the Internet should pass GE 0/2. ● If the GE 0/1 link is disconnected, the data streams on the GE 0/1 interface are switched to the GE 0/2 interface. Vice versa.
Configuration Steps	● Configure two ACLs to match packets from subnets 1 and 2 respectively. ● Set a policy to set the next hops for packets from subnet 1 to GE0/1 and GE0/2. (Pay attention to the configuration sequence.) ● Set a policy to set the next hops for packets from subnet 2 to GE0/2 and GE0/1. (Pay attention to the configuration sequence.) ● Apply the policy to GE 0/3. ● Set PBR to implement redundant backup among multiple next hops. During redundant backup, based on the configuration sequence, the first next hop takes effect first.
	DEV1(config)# ipv6 access-list net1 DEV1(config-ipv6-acl)# permit ipv6 2003::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# ipv6 access-list net2 DEV1(config-ipv6-acl)# permit ipv6 2004::/64 any

```
DEV1(config-ipv6-acl)# exit
DEV1(config)# route-map RM_FOR_PBR 30
DEV1(config-route-map)# match ipv6 address net1
DEV1(config-route-map)# set ipv6 next-hop 2001::1
DEV1(config-route-map)# set ipv6 next-hop 2002::1
DEV1(config-route-map)# exit
DEV1(config)# route-map RM_FOR_PBR 40
DEV1(config-route-map)# match ipv6 address net2
DEV1(config-route-map)# set ipv6 next-hop 2002::1
DEV1(config-route-map)# set ipv6 next-hop 2001::1
DEV1(config-route-map)# exit
DEV1(config)# interface GigabitEthernet 0/3
DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_FOR_PBR
DEV1(config-if-GigabitEthernet 0/3)# exit
DEV1(config)# ipv6 policy redundance
```

Verification

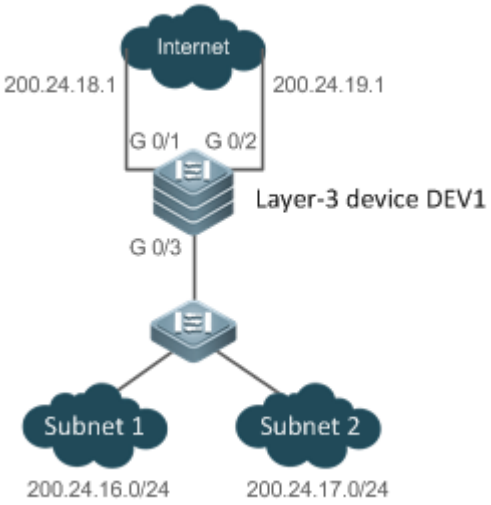
- Check the configurations of IPv6 PBR.
- Check the configurations of the route map.
- Check the configurations of an ACL.

```
DEV1# show ipv6 policy
Interface                      Route map
GigabitEthernet 0/3            RM_FOR_PBR
```

```
DEV1# show route-map
route-map RM_FOR_PBR, permit, sequence 11
  Match clauses:
    ipv6 address net1
  Set clauses:
    ipv6 next-hop 2001::1 2002::1
route-map RM_FOR_PBR, permit, sequence 21
  Match clauses:
    ipv6 address net2
  Set clauses:
```

	ipv6 next-hop 2002::1 2001::1
	DEV1# show access-lists ipv6 access-list net1 10 permit ipv6 2003::/64 any (0 packets matched) ipv6 access-list net2 10 permit ipv6 2004::/64 any (0 packets matched)

Configuring correlation between IPv4 PBR and Track

Scenario **Figure 3-4**	
	The layer-3 device DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24 whereas the network segment where subnet 2 resides is 200.24.17.0/24. DEV 1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.
	● DEV1 can fast detect a faulty output link and switch to a backup link.
Configuration Steps	When configuring IPv4 PBR and selecting an output link based on source addresses of the packets, add or modify the following configurations (red fields): ● Set two Track objects and track the accessibility of the next hops of the two output interfaces. ● When configuring a policy, set the correlation between the next hops and the Track objects.
DEV1	DEV1(config)# ip access-list extended 101 DEV1(config-ip-acl)# permit ip 200.24.16.0 0.0.0.255 any

```
DEV1(config-ip-acl)# exit
DEV1(config)# ip access-list extended 102
DEV1(config-ip-acl)# permit ip 200.24.17.0 0.0.0.255 any
DEV1(config-ip-acl)# exit
DEV1(config)#ip rns 1
DEV1(config-ip-rns)#icmp-echo 200.24.18.1
DEV1(config)#ip rns schedule 1 start-time now life forever
DEV1(config)#track 1 rns 1
DEV1(config)#ip rns 2
DEV1(config-ip-rns)#icmp-echo 200.24.19.1
DEV1(config)#ip rns schedule 2 start-time now life forever
DEV1(config)#track 2 rns 2
DEV1(config)# route-map RM_FOR_PBR 10
DEV1(config-route-map)# match ip address 101
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
DEV1(config-route-map)# exit
DEV1(config)# route-map RM_FOR_PBR 20
DEV1(config-route-map)# match ip address 102
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2
DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1
DEV1(config-route-map)# exit
DEV1(config)# interface GigabitEthernet 0/3
DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR
DEV1(config-if-GigabitEthernet 0/3)# exit
DEV1(config)# ip policy redundance
```

Verification

- Check whether the Track objects are up.

DEV1

```
DEV1#show track
Track 1
  Reliable Network Service 1
  The state is Up
```

	1 change, current state last: 120 secs Delay up 30 secs, down 50 secs Track 2 Reliable Network Service 2 The state is Up 1 change, current state last: 130 secs Delay up 30 secs, down 50 secs

Configuring IPv4 PBR and transferring global packets to a VRF for forwarding

	VRF1 and VRF2 are available on the device. Select VRFs for forwarding IPv4 packets received on GE0/3: ● Forward IPv4 packets from subnet 1 in VRF 1. ● Forward IPv4 packets from subnet 2 in VRF 2.
Configuration Steps	● Configure a single-protocol VRF (or multi-protocol VRF to enable the IPv4 address family). ● Configure ACL1: the source addresses of IPv4 packets belong to subnet 1. ● Configure ACL2: the source addresses of IPv4 packets belong to subnet 2. ● Set policy 10 in a route map: forward packets matching ACL 1 in VRF1. ● Set policy 20 in a route map: forward packets matching ACL 2 in VRF2. ● Apply the route map to GE 0/3. ● Redirect the host route and direct route on GE 0/3 to the VRF.
Single-protocol VRF	DEV1 (config)# ip vrf VRF1 DEV1 (config)# ip vrf VRF2 DEV1 (config)# access-list 1 permit 192.168.195.0 0.0.0.255 DEV1 (config)# access-list 2 permit 192.168.196.0 0.0.0.255 DEV1 (config)# route-map PBR-VRF-Selection permit 10 DEV1 (config-route-map)# match ip address 1 DEV1 (config-route-map)# set vrf VRF1 DEV1 (config-route-map)# exit DEV1 (config)# route-map PBR-VRF-Selection permit 20 DEV1 (config-route-map)# match ip address 2 DEV1 (config-route-map)# set vrf VRF2 DEV1 (config-route-map)# exit DEV1 (config)# interface GigabitEthernet 0/3

	DEV1 (config-if-GigabitEthernet 0/3)# ip policy route-map PBR-VRF-Selection DEV1 (config-if-GigabitEthernet 0/3)# ip address 192.168.195.1 255.255.255.0 DEV1 (config-if-GigabitEthernet 0/3)# ip vrf receive VRF1 DEV1 (config-if-GigabitEthernet 0/3)# ip vrf receive VRF2 DEV1 (config-if-GigabitEthernet 0/3)# exit
Multi-protocol VRF	DEV1 (config)# vrf definition VRF1 DEV1 (config-vrf)# address-family ipv4 DEV1 (config-vrf-af)# exit-address-family DEV1 (config-vrf)# exit DEV1 (config)# vrf definition VRF2 DEV1 (config-vrf)# address-family ipv4 DEV1 (config-vrf-af)# exit-address-family DEV1 (config-vrf)# exit DEV1 (config)# access-list 1 permit 192.168.195.0 0.0.0.255 DEV1 (config)# access-list 2 permit 192.168.196.0 0.0.0.255 DEV1 (config)# route-map PBR-VRF-Selection permit 10 DEV1 (config-route-map)# match ip address 1 DEV1 (config-route-map)# set vrf VRF1 DEV1 (config-route-map)# exit DEV1 (config)# route-map PBR-VRF-Selection permit 20 DEV1 (config-route-map)# match ip address 2 DEV1 (config-route-map)# set vrf VRF2 DEV1 (config-route-map)# exit DEV1 (config)# interface GigabitEthernet 0/3 DEV1 (config-if-GigabitEthernet 0/3)# ip policy route-map PBR-VRF-Selection DEV1 (config-if-GigabitEthernet 0/3)# ip address 192.168.195.1 255.255.255.0 DEV1 (config-if-GigabitEthernet 0/3)# vrf receive VRF1 DEV1 (config-if-GigabitEthernet 0/3)# vrf receive VRF2 DEV1 (config-if-GigabitEthernet 0/3)# exit

Verification	● Check the configurations of IPv4 PBR. ● Check the configurations of the route map. ● Check the configurations of the ACLs.
	DEV1# show ip policy Interface Route map GigabitEthernet 0/3 PBR-VRF-Selection
	DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: ip address 1 Set clauses: vrf VRF1 route-map PBR-VRF-Selection, permit, sequence 20 Match clauses: ip address 2 Set clauses: vrf VRF2
	DEV1# show access-lists ip access-list standard 1 10 permit 192.168.195.0 0.0.0.255 ip access-list standard 2 10 permit 192.168.196.0 0.0.0.255

Configuring IPv6 PBR and transferring global packets to a VRF for forwarding

	VRF1 and VRF2 are available on the device. Select a VRF for forwarding IPv6 packets received on GE0/3: ● Forward IPv6 packets from subnet 1 in VRF 1. ● Forward IPv6 packets from subnet 2 in VRF 2.
Configuration Steps	● Configure multi-protocol VRFs and enable the IPv6 address family. ● Configure ACL net1: the source addresses of IPv6 packets belong to subnet 1. ● Configure ACL net2: the source addresses of IPv6 packets belong to subnet 2. ● Set policy 10 in a route map: forward packets matching ACL 1 in VRF1. ● Set policy 20 in a route map: forward packets matching ACL 2 in VRF2. ● Apply the route map to GE 0/3.

	● Redirect the host route and direct route on GE 0/3 to the VRF.
Multi-protocol VRF	DEV1(config)# vrf definition VRF1 DEV1(config-vrf)# address-family ipv6 DEV1(config-vrf-af)# exit-address-family DEV1(config-vrf)# exit DEV1(config)# vrf definition VRF2 DEV1(config-vrf)# address-family ipv6 DEV1(config-vrf-af)# exit-address-family DEV1(config-vrf)# exit DEV1(config)# ipv6 access-list net1 DEV1(config-ipv6-acl)# permit ipv6 1000::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# ipv6 access-list net2 DEV1(config-ipv6-acl)# permit ipv6 2000::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# route-map PBR-VRF-Selection permit 10 DEV1(config-route-map)# match ipv6 address net1 DEV1(config-route-map)# set vrf VRF1 DEV1(config-route-map)# exit DEV1(config)# route-map PBR-VRF-Selection permit 20 DEV1(config-route-map)# match ipv6 address net2 DEV1(config-route-map)# set vrf VRF2 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map PBR-VRF-Selection DEV1(config-if-GigabitEthernet 0/3)# vrf receive VRF1 DEV1(config-if-GigabitEthernet 0/3)# vrf receive VRF2 DEV1(config-if-GigabitEthernet 0/3)# exit
Verification	● Check the configurations of IPv6 PBR. ● Check the configurations of the route map.

	● Check the configurations of the ACLs.
	DEV1# show ipv6 policy Interface Route map GigabitEthernet 0/3 PBR-VRF-Selection
	DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: ip address 1 ipv6 address net1 Set clauses: vrf VRF1 route-map PBR-VRF-Selection, permit, sequence 20 Match clauses: ip address 2 ipv6 address net2 Set clauses: vrf VRF2
	DEV1# show access-lists ipv6 access-list net1 10 permit ipv6 1000::/64 any ipv6 access-list net2 10 permit ipv6 2000::/64 any

Common Errors

- A route map is used when PBR is configured but the route map does not exist.
- An ACL is used when a route map is configured but the ACL does not exist.
- A VRF is used when a route map is configured but the VRF does not exist.
- When multi-protocol VRF is configured, the IPv4 or IPv6 address family is not enabled.
- When PBR is used for VRF transfer, the host route and direct route on the interface are not redirected to the VRF.

3.4.2 Setting Redundant Backup or Load Balancing

Configuration Effect

- Using multiple next hops in the mutual backup mode can enhance the network reliability.
- Implementing load balancing among multiple next hops can expand the network bandwidth.

Notes

- The basic functions of PBR must be configured.
- Redundant backup and load balancing are effective only for the next hops set by the following **set** commands.

Command	Description
set ip next-hop	Configures the next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.
set ip default next-hop	Configures the default next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.
set ipv6 next-hop	Configures the next hop of IPv6 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.
set ipv6 default next-hop	Configures the default next hop of IPv6 packets. This command carries the *weight* parameter, which is used to set the weight of the WCMP. The default value is 1.
set ip next-hop recursive	Configures the recursive next hop of IPv4 packets. Only one command can be configured for a route map and packets can recur to multiple next hops (up to 32 next hops) of a static or dynamic ECMP route. The redundant backup or load balancing mode for recurring to multiple next hops is also determined by the **ip policy** { **redundance** | **load-balance** } command.

Up to eight next hops can be set for WCMP whereas up to 32 next hops can be set for ECMP.

Configuration Steps

Setting whether IPv4 PBR implements redundant backup or load balancing among multiple next hops

- If load balancing needs to be implemented among multiple next hops, this configuration needs to be performed.
- If load balancing is configured at present, you also need to perform this configuration to reset redundant backup.
- This configuration is effective for all PBRs configured on a device.

Command	**ip policy** { **redundance** | **load-balance** }
Parameter Description	redundance: Indicates redundant backup. load-balance: Indicates load balancing.
Defaults	Redundant backup is configured by default.
Command Mode	Global configuration mode
Usage Guide	If redundant backup is selected, the first next hop takes effect based on the configuration sequence. If load balancing is selected, all next hops take effect at the same time and share traffic by weight.

Setting whether Ipv6 PBR implements redundant backup or load balancing among multiple next hops

- If load balancing needs to be implemented among multiple next hops, this configuration needs to be performed.
- If load balancing is configured at present, you also need to perform this configuration to reset redundant backup.

- This configuration is effective for all PBRs configured on a device.

Command	**ipv6 policy** { **redundance** | **load-balance** }
Parameter Description	redundance: Indicates redundant backup. load-balance: Indicates load balancing.
Defaults	Redundant backup is configured by default.
Command Mode	Global configuration mode
Usage Guide	If redundant backup is selected, the first next hop takes effect based on the configuration sequence. If load balancing is selected, all next hops take effect at the same time and share traffic by weight.

Verification

- Check whether redundant backup or load balancing is implemented among multiple next hops.

Checking whether IPv4 PBR implements redundant backup or load balancing among multiple next hops

Command	**show ip policy** [*route-map-name*]
Parameter Description	***route-map-name*: Specifies a route map.**
Command Mode	Privilege, global and interface configuration modes
Usage Guide	See the following example and focus on the red field. `ruijie# show ip policy` `Banlance mode: redundance` `Interface Route map` `local test` `GigabitEthernet 0/3 test`

Checking whether IPv6 PBR implements redundant backup or load balancing among multiple next hops

Command	**show ipv6 policy** [*route-map-name*]
Parameter Description	***route-map-name***: Specifies a route map.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	See the following example and focus on the red field. `ruijie#show ipv6 policy` `Banlance mode: redundance` `Interface Route map` `VLAN 1 RM_for_Vlan_1`

	VLAN 2 RM_for_Vlan_2

Configuration Example

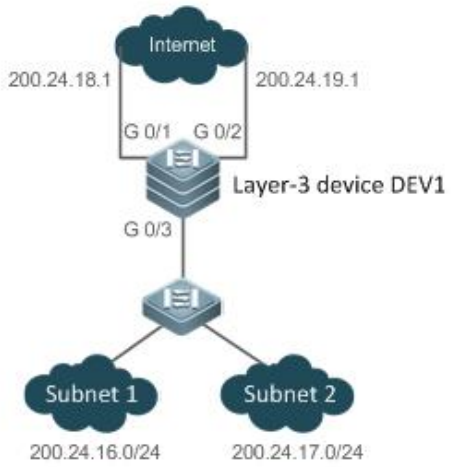
Configuring IPv4 PBR to implement redundant backup among multiple next hops

See the preceding example: Configuring IPv4 PBR and selecting an output link based on source addresses of packets

Configuring IPv6 PBR to implement redundant backup among multiple next hops

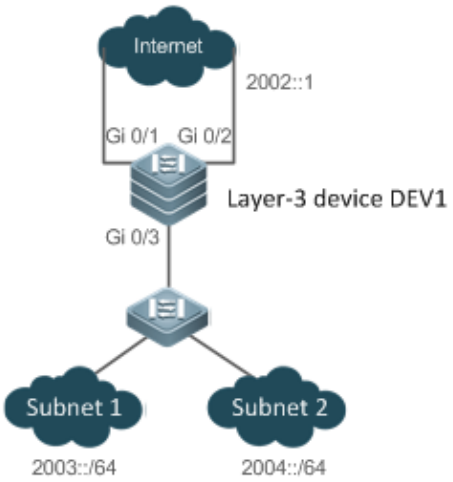
See the preceding example: Configuring IPv6 PBR and selecting an output link based on source addresses of packets

Configuring IPv4 PBR to implement load balancing among multiple next hops

Scenario **Figure 3-5**	
	The layer-3 device DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24 whereas the network segment where subnet 2 resides is 200.24.17.0/24. DEV 1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.
	This LAN has two output interfaces for connecting the Internet. The requirements are as follows: The traffic is equally shared by GE0/1 and GE0/2.
Configuration Steps	● Configure basic functions of PBR. Specify multiple next hops. ● Set the load balancing mode.
	DEV1(config)# route-map RM_LOAD_PBR 10 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit

	DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_LOAD_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy load-balance
Verification	● Check the configurations of IPv4 PBR. ● Check the configurations of the route map.
	DEV1# show ip policy Balance mode: load-balance Interface Route map GigabitEthernet 0/3 RM_LOAD_PBR
	DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: Set clauses: ip next-hop 200.24.18.1 8 ip next-hop 200.24.19.1 8

Configuring IPv6 PBR to implement load balancing among multiple next hops

Scenario **Figure 3-6**	
	DEV 1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 2003::/64 whereas the network segment where subnet 2 resides is 2004::/64. DEV1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 2001::1/64 and 2002::1/64.

	This LAN has two output interfaces for connecting the Internet. The requirements are as follows: The traffic is equally shared by GE0/1 and GE0/2.
Configuration Steps	● Configure basic functions of PBR. Specify multiple next hops. ● Set the load balancing mode.
	DEV1(config)# route-map RM_LOAD_PBR 20 DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_LOAD_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ipv6 policy load-balance
Verification	● Check the configurations of IPv6 PBR. ● Check the configurations of the route map.
	DEV1# show ipv6 policy Balance mode: load-balance Interface Route map GigabitEthernet 0/3 RM_LOAD_PBR DEV1# show route-map route-map PBR-VRF-Selection, permit, sequence 10 Match clauses: Set clauses: ipv6 next-hop 2001::1 ipv6 next-hop 2002::1

3.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command

Clears the statistics about packets forwarded by IPv4 PBR.	**clear ip pbr statistics** [**interface** *if-name* | **local**]
Clears the statistics about packets forwarded by IPv6 PBR.	**clear ipv6 pbr statistics** [**interface** *if-name* | **local**]

Displaying

Description	Command
Displays the configurations of IPv4 PBR.	**show ip policy**
Displays the configurations of IPv6 PBR.	**show ipv6 policy**
Displays the configurations of a route map.	**show route-map** [*name*]
Displays the configurations of an ACL.	**show access-list**
Displays the correlation between IPv4 PBR and BFD.	**show ip pbr bfd**
Displays the correlation between IPv6 PBR and BFD.	**show ipv6 pbr bfd**
Displays the routing information of IPv4 PBR.	**show ip pbr route** [**interface** *if-name* | **local**]
Displays the routing information of IPv6 PBR.	**show ipv6 pbr route** [**interface** *if-name* | **local**]
Displays a route map used by IPv4 PBR.	**show ip pbr route-map** *rmap-name*
Displays a route map used by IPv6 PBR.	**show ipv6 pbr route-map** *rmap-name*
Displays the statistics about IPv4 PBR.	**show ip pbr statistics** [**interface** *if-name* | **local**]
Displays the statistics about IPv6 PBR.	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs PBR errors.	**debug pbr error**
Debugs PBR events.	**debug pbr events**
Debugs multiple service cards supported by PBR.	**debug pbr ms**
Debugs PBR message communication.	**debug pbr msg**
Debugs interaction between PBR and NSM.	**debug pbr nsm**
Debugs packet forwarding of PBR.	**debug pbr packet**
Debugs PBR GR.	**debug pbr restart**

4 Configuring RIP

4.1 Overview

Routing Information Protocol (RIP) is a unicast routing protocol applied on IPv4 networks. RIP-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within the autonomous system (AS) and is applicable to small-sized networks whose longest path involves less than 16 hops.

Protocols and Standards

- RFC1058: Defines RIPv1.
- RFC2453: Defines RIPv2.

4.2 Applications

Application	Description
Basic RIP Application	The routing information is automatically maintained through RIP on a small-sized network.

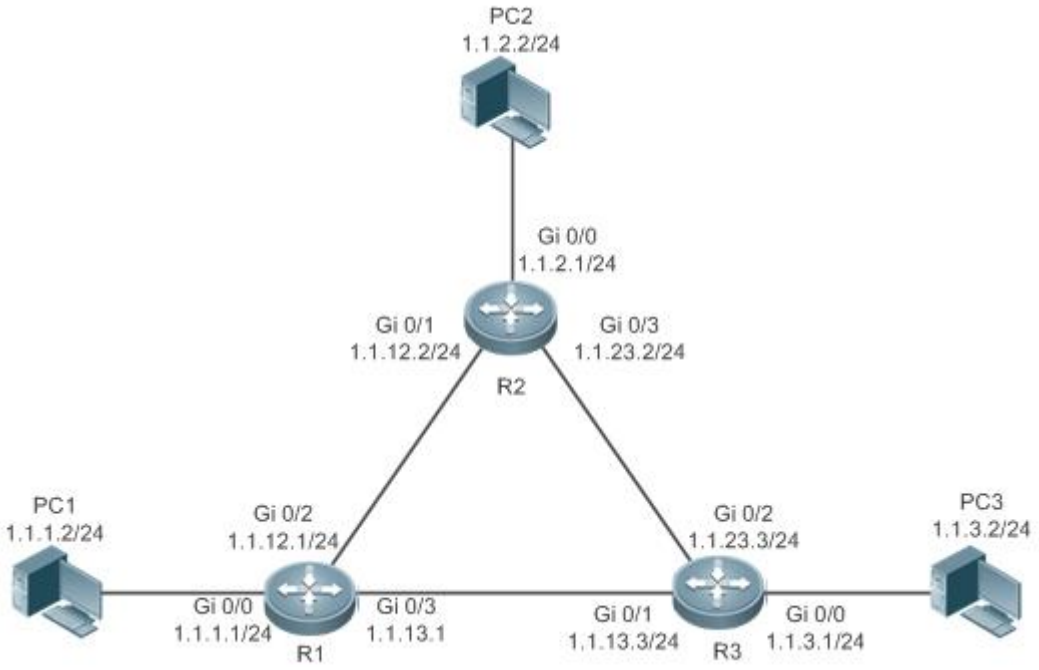
4.2.1 Basic RIP Application

Scenario

On a network with a simple structure, you can configure RIP to implement network interworking. Configuring RIP is simpler than configuring other IGP protocols like Open Shortest Path First (OSPF). Compared with static routes, RIP can dynamically adapt to the network structure changes and is easier to maintain.

As shown in Figure 4-1, to implement interworking between PC1, PC2, and PC3, you can configure RIP routes on R1, R2, and R3.

Figure 4-1



Deployment

- Configure IP addresses and gateways on three PCs.
- Configure IP addresses and subnet masks on three routers.
- Configure RIP on three routers.

4.3 Features

Basic Concepts

IGP and EGP

IGP runs within an AS. For example, RIP is a type of IGP.

Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

Classful Routing Protocol and Classless Routing Protocol

Protocols can be classified based on the type of routes supported:

- Classful routing protocol: It supports classful routes. For example, RIPv1 is a classful routing protocol.
- Classless routing protocol: It supports classless routes. For example, RIPv2 is a classless routing protocol.

Overview

Feature	Description

Feature	Description
RIPv1 and RIPv2	RIP is available in two versions: RIPv1 and RIPv2.
Exchanging Routing Information	By exchanging routing information, RIP-enabled devices can automatically obtain routes to a remote network and update the routes in real time.
Routing Algorithm	RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIP uses functions, such as split horizon and poison reverse, to avoid route loops.
Security Measures	RIP uses functions, such as authentication and source address verification, to ensure protocol security.
Reliability Measures	RIP uses function graceful restart (GR) to enhance reliability of the protocol.

4.3.1 RIPv1 and RIPv2

Two RIP versions are available: RIPv1 and RIPv2.

Working Principle

RIPv1

RIPv1 packets are broadcast. The broadcast address is 255.255.255.255, and the UDP port ID is 520. RIPv1 cannot identify the subnet mask, and supports only classful routes.

RIPv2

RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask, and supports classless routes, summarized route, and supernetting routes. RIPv2 supports plain text authentication and message digest 5 (MD5) authentication.

Related Configuration

Enabling the RIP Process

The RIP process is disabled by default.

Run the **router rip** command to enable the RIP process.

You must enable the RIP process on a device; otherwise, all functions related to RIP cannot take effect.

Running RIP on an Interface

By default, RIP does not run on an interface.

Run the **network** command to define an address range. RIP runs on interfaces that belong to this address range.

After RIP runs on an interface, RIP packets can be exchanged on the interface and RIP can learn routes to the network segments directly connected to the device.

Defining the RIP Version

By default, an interface receives RIPv1 and RIPv2 packets, and sends RIPv1 packets.

Run the **version** command to define the version of RIP packets sent or received on all interfaces.

Run the **ip rip send version** command to define the version of RIP packets sent on an interface.

Run the **ip rip receive version** command to define the version of RIP packets received on an interface.

> If the versions of RIP running on adjacent routers are different, the RIPv1-enabled router will learn incorrect routes.

Preventing an Interface from Sending or Receiving Packets

By default, a RIP-enabled interface is allowed to send and receive RIP packets.

Run the **no ip rip receive enable** command to prevent an interface from receiving RIP packets.

Run the **no ip rip send enable** command to prevent an interface from sending RIP packets.

Run the **passive-interface** command to prevent an interface from sending broadcast or multicast RIP packets.

Configuring the Mode for Sending RIP Packets

By default, broadcast RIPv1 packets and multicast RIPv2 are sent.

Run the **ip rip v2-broadcast** command to send broadcast RIPv2 packets on an interface.

Run the **neighbor** command to send unicast RIP packets to a specified neighbor router.

4.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIP is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router returns a response packet containing the local routing table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIP. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighbor routers. One update packet contains at most 25

routes. Therefore, a lot of update packets may be required to send the entire routing table. You can set the sending delay between update packets to avoid loss of routing information.

For every non-local route, if the route is not updated within 180s (invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (flush timer), the route is deleted from the routing table.

Triggered Updates

After the triggered updates function is enabled, periodical update is automatically disabled. When routing information changes on a router, the router immediately sends routes related to the change (instead of the complete routing table) to the neighbor router, and use the acknowledgment and retransmission mechanisms to ensure that the neighbor router receives the routes successfully. Compared with periodical update, triggered updates help reduce flooding and accelerates route convergence.

Events that can trigger update include router startup, interface status change, changes in routing information (such as the metric), and reception of a request packet.

Route Summarization

When sending routing information to a neighbor router, the RIP-enabled router summarizes subnet routes that belong to the same classful network into a route, and sends the route to the neighbor router. For example, summarize 80.1.1.0/24 (metric=2) and 80.1.2.0/24 (metric=3) into 80.0.0.0/8 (metric=2), and set the metric of the summarized route to the optimum metric.

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange.

Supernetting Route

If the subnet mask length of a route is smaller than the natural mask length, this route is called supernetting route. For example, in the 80.0.0.0/6 route, as 80.0.0.0 is a Class A network address and the natural mask is 8 bits, 80.0.0.0/6 route is a supernetting route.

Only RIPv2 supports supernetting routes.

Default Route

In the routing table, a route to the destination network 0.0.0.0/0 is called default route.

The default route can be learned from a neighbor router, or sent to a neighbor router.

Route Redistribution

For RIP, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

External routes (excluding the default route) can be redistributed to RIP and advertised to neighbors.

Route Filtering

Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

Related Configuration

Sending Delay Between Update Packets

By default, the update packets are sent continuously without any delay.
Run the **output-delay** command to set the sending delay between update packets.

RIP Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Run the **timers basic** command to modify durations of the RIP timers.

Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.

The durations of RIP timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIP timers.

Triggered Updates

By default, periodical update is enabled.

Run the **ip rip triggered** command to enable triggered updates on the interface and disable periodical update.

Run the **ip rip triggered retransmit-timer** command to modify the retransmission interval of update packets. The default value is 5s.

Run the **ip rip triggered retransmit-count** command to modify the maximum retransmission times of update packets. The default value is 36.

Route Summarization

By default, route summarization is automatically enabled if an interface is allowed to send RIPv2 packets.

Run the **no auto-summary** command to disable route summarization.

Run the **ip rip summary-address** command to configure route summarization on an interface.

Supernetting Route

By default, supernetting routes can be sent if an interface is allowed to send RIPv2 packets.

Run the **no ip rip send supernet-routes** command to prevent the sending of supernetting routes.

Default Route

Run the **ip rip default-information** command to advertise the default route to neighbors on an interface.

Run the **default-information originate** command to advertise the default route to neighbors from all interfaces.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIP and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.

Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

4.3.3 Routing Algorithm

RIP is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

Working Principle

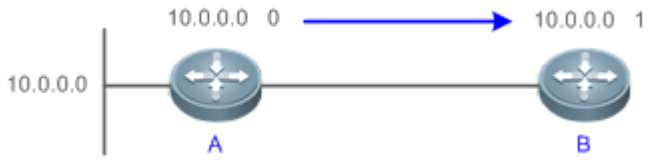
Distance-Vector Algorithm

RIP is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance (metric). The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.

RIP uses the hop count to evaluate the distance (metric) to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through the router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIP stipulates that the metric must be an integer between 0 and 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIP cannot be applied on a large-scale network.

As shown in Figure 4-, Router A is connected to the network 10.0.0.0. Router B obtains the route (10.0.0.0,0) from Router A and adds the metric 1 to the route to obtain its own route ((10.0.0.0,1), and the next hop points to Router A.

Figure 4-2

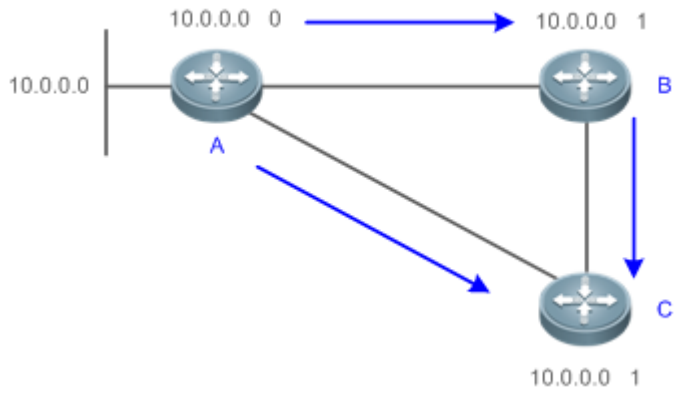


Selecting the Optimum Route

RIP selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in Figure 4-, Router A is connected to the network 10.0.0.0. Router C obtains the route (10.0.0.0,0) from Router A and the route (10.0.0.0,1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Router A.

Figure 4-3



When routes coming from different sources exist on a router, the route with the smallest distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
RIP route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIP route is 120.

Run the **distance** command to modify the distance of a RIP route.

Modifying the Metric

For a RIP route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. For a RIP router that is manually configured (default route or redistributed route), the default metric is 1.

Run the **offset-list in** command to increase the metric of a received RIP route.

Run the **offset-list out** command to increase the metric of a sent RIP route.

Run the **default-metric** command to modify the default metric of a redistributed route.

Run the **redistribute** command to modify the metric of a route when the route is redistributed.

Run the **default-information originate** command to modify the metric of a default route when the default route is introduced.

Run the **ip rip default-information** command to modify the metric of a default route when the default route is created.

4.3.4 Avoiding Route Loops

RIP uses functions, such as split horizon and poison reverse, to avoid route loops.

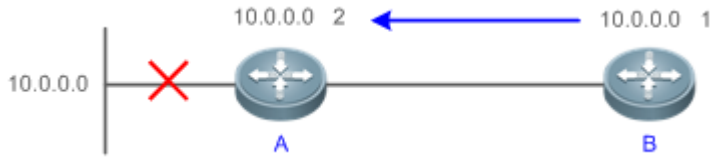
Working Principle

Route Loop

A RIP route loop occurs due to inherent defects of the distance-vector algorithm.

As shown in Figure 4-, Router A is connected to the network 10.0.0.0, and sends an update packet every 30s. Router B receives the route 10.0.0.0 from Router A every 30s. If Router A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 10.0.0.0, Router B determines that the route to 10.0.0.0 is valid within 180s and uses the Update packet to send this route to Router A. As the route to 10.0.0.0 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 10.0.0.0 through Router A, and Router A determines that data can reach 10.0.0.0 through Router B. In this way, a route loop is formed.

Figure 4-4



Split Horizon

Split horizon can prevent route loops. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

As shown in Figure 4-, after split horizon is enabled on the interface between Router A and Router B, Router B will not send the route 10.0.0.0 back to Router A. Router B will learn 180s later that 10.0.0.0 is not reachable.

Figure 4-5

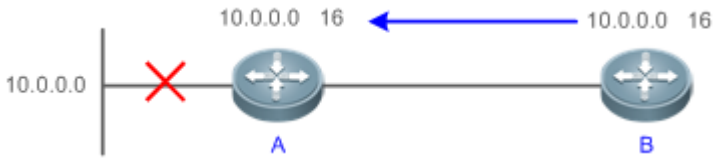
Poison Reverse

Poison reverse can also prevent route loops. Compared with slit horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in Figure 4-, after learning the route 10.0.0.0 from Router A, Router B sets the metric of this route to 16 and sends the route back to Router A. After this route becomes invalid, Router B advertises the route 10.0.0.0 (metric = 16) to Router A to accelerate the process of deleting the route from the routing table.

Figure 4-6



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no ip rip split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **ip rip split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

4.3.5 Security Measures

RIP uses functions, such as authentication and source address verification, to ensure protocol security.

Working Principle

Authentication

RIPv2 supports authentication, but RIPv1 does not.

After authentication is enabled on an interface, the routing information cannot be exchanged between adjacent devices if authentication fails. The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain.

RIPv2 supports plain text authentication and MD5 authentication.

Source Address Verification

When a RIP-enabled device receives an Update packet, it checks whether the source IP address in the packet and the IP address of the inbound interface are in the same network segment. If not, the device drops the packet. Source address verification is used to ensure that RIP routing information is exchanged only between adjacent routing devices.

- On an unnumbered IP interface, source address verification is not performed (not configurable).
- If the triggered updates function is enabled, source address verification is automatically enabled (not configurable).
- If split horizon is disabled, source address verification is automatically enabled (not configurable).

Related Configuration

Authentication

By default, authentication is disabled.

Run the **ip rip authentication mode text** command to enable plain text authentication on an interface.

Run the **ip rip authentication mode md5** command to enable MD5 authentication on an interface.

Run the **ip rip authentication text-password** command to set the password for plain text authentication on an interface.

Run the **ip rip authentication key-chain** command to reference the key in the configured key chain as the authentication key on an interface.

Source Address Verification

By default, source address verification is enabled.

Run the **no validate-update-source** command to disable source address verification.

4.3.6 Reliability Measures

RIP uses function GR to enhance reliability of the protocol.

Working Principle

GR

GR ensures uninterrupted data transmission when the protocol is restarted. If RIP is restarted on a GR-enabled device, the forwarding table before restart will be retained and a request packet will be sent to the neighbor so that the route can be learned again. During the GR period, RIP completes re-convergence of the route. After the GR period expires, RIP updates the forwarding entry and advertises the routing table to the neighbor.

Related Configuration

GR

By default, GR is disabled.

Run the **graceful-restart** command to enable the GR function.

4.4 Configuration

Configuration	Description and Command	
Configuring RIP Basic Functions	(Mandatory) It is used to build a RIP routing domain.	
	router rip	Enables a RIP routing process and enters routing process configuration mode.
	network	Runs RIP on interfaces in the specified address range.

Configuration	Description and Command	
	version	Defines the RIP version.
	ip rip split-horizon	Enables split horizon or poison reverse on an interface.
	passive-interface	Configures a passive interface.
Controlling Interaction of RIP Packets	(Optional) This configuration is required if you wish to change the default mechanism for sending or receiving RIP packets.	
	neighbor	Sends unicast RIP packets to a specified neighbor.
	ip rip v2-broadcast	Sends broadcast RIPv2 packets on an interface.
	ip rip receive enable	Allows the interface to receive RIP packets.
	ip rip send enable	Allows the interface to send RIP packets.
	ip rip send version	Defines the version of RIP packets sent on an interface.
	ip rip receive version	Defines the version of RIP packets received on an interface.
Enabling Triggered Updates	Optional.	
	ip rip triggered	Enables triggered updates on an interface.
Enabling Source Address Verification	Optional.	
	validate-update-source	Enables source address verification.
Enabling Authentication	(Optional) Only RIPv2 supports authentication.	
	ip rip authentication mode	Enables authentication and sets the authentication mode on an interface.
	ip rip authentication text-password	Configures the password for plain text authentication on an interface.
	ip rip authentication key-chain	Configures the authentication key chain on an interface.
Enabling Route Summarization	(Optional) Only RIPv2 supports route summarization.	
	auto-summary	Enables automatic summarization of RIP routes.
	ip rip summary-address	Configures route summarization on an interface.
Enabling Supernetting Routes	(Optional) Only RIPv2 supports supernetting routes.	
	ip rip send supernet-routes	Enables advertisement of RIP supernetting routes on an interface
Advertising the Default Route or External Routes	Optional.	
	ip rip default-information	Advertises the default route to neighbors on an interface.

Configuration	Description and Command	
	default-information originate	Advertises the default route to neighbors.
	redistribute	Redistributes routes and advertises external routes to neighbors.
Setting Route Filtering Rules	⚠ Optional.	
	distribute-list in	Filters the received RIP routing information.
	distribute-list out	Filters the sent RIP routing information.
Modifying Route Selection Parameters	⚠ Optional.	
	distance	Modifies the administrative distance (AD) of a RIP route.
	offset-list	Increases the metric of a received or sent RIP route.
	default-metric	Configures the default metric of an external route redistributed to RIP.
Modifying Timers	⚠ Optional.	
	timers basic	Modifies the update timer, invalid timer, and flush timer.
	output-delay	Sets the sending delay between RIP route update packets.
Enabling GR	⚠ Optional.	
	graceful-restart	Configures the GR restarter capability.

4.4.1 Configuring RIP Basic Functions

Configuration Effect

- Build a RIP routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIP.

Notes

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

Configuration Steps

↘ Enabling a RIP Routing Process

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.

↘ Associating with the Local Network

- Mandatory.
- Unless otherwise required, this configuration must be performed on every router in the RIP routing domain.
- Unless otherwise required, the local network associated with RIP should cover network segments of all L3 interfaces.

Defining the RIP Version

- If RIPv2 functions (such as the variable length subnet mask and authentication) are required, enable the RIPv2.
- Unless otherwise required, you must define the same RIP version on every router.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access (NBMA) network, such as FR and X.25; otherwise, some devices may fail to learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- If you want to suppress Update packets on a RIP interface, configure the interface as a passive interface.
- Use the passive interface to set the boundary of the RIP routing domain. The network segment of the passive interface belongs to the RIP routing domain, but RIP packets cannot sent over the passive interface.
- If RIP routes need to be exchanged on an interface (such as the router interconnect interface) in the RIP routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIP.

Related Commands

Enabling a RIP Routing Process

Command Syntax	**router rip**
Parameter Description	N/A
Command Mode	Global configuration mode

Configuration Usage	This command is used to create a RIP routing process and enter routing process configuration mode.

Associating with the Local Network

Command Syntax	**network** *network-number* [*wildcard*]
Parameter Description	*network-number*: Indicates the number of a network. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	RIP can run and learn direct routes and RIP packets can be exchanged only on an interface covered by **network**. If **network** 0.0.0.0 255.255.255.255 is configured, all interfaces are covered. If *wildcard* is not configured, the classful address range is used by default, that is, the interfaces whose addresses fall into the classful address range participate in RIP operations.

Defining the RIP Version

Command Syntax	**version** { **1** | **2** }
Parameter Description	**1**: Indicates RIPv1. **2**: Indicates RIPv2.
Command Mode	Global configuration mode
Configuration Usage	This command takes effect on the entire router. You can run this command to define the version of RIP packets sent or received on all interfaces.

Enabling Split Horizon

Command Syntax	**ip rip split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates poison reverse.
Command Mode	Interface configuration mode
Configuration Usage	After poison reverse is enabled, split horizon is automatically disabled.

Configuring a Passive Interface

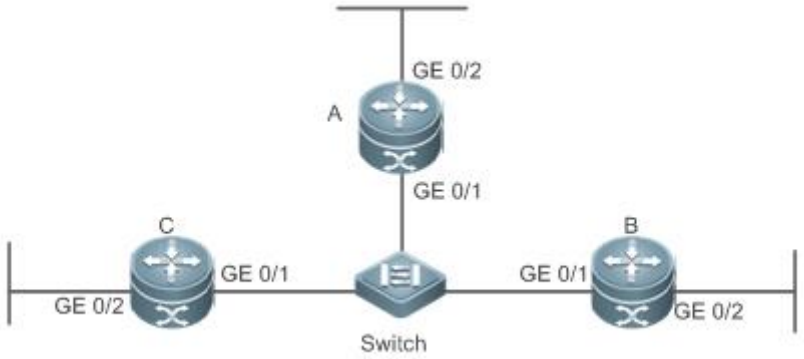
Command Syntax	**passive-interface** { **default** | *interface-type interface-num* }
Parameter	**default:** Indicates all interfaces.

Description	***interface-type interface-num*:** Specifies an interface.
Command Mode	Routing process configuration mode
Configuration Usage	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command to cancel the interfaces used for interconnection between routers in the domain.

Configuration Example

Building a RIP Routing Domain

Scenario
Figure 4-7



Remarks	The interface IP addresses are as follows: A: GE0/1 110.11.2.1/24 GE0/2 155.10.1.1/24 B: GE0/1 110.11.2.2/24 GE0/2 196.38.165.1/24 C: GE0/1 110.11.2.3/24 GE0/2 117.102.0.1/16

Configuration Steps

- Configure the interface IP addresses on all routers.
- Configure the RIP basic functions on all routers.

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0
A(config)# router rip
A(config-router)# version 2
A(config-router)# network 0.0.0.0 255.255.255.255
A(config-router)# passive-interface default
A(config-router)# no passive-interface GigabitEthernet 0/1
```

B

```
B# configure terminal
```

	B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)# exit B(config)# router rip B(config-router)# version 2 B(config-router)# network 0.0.0.0 255.255.255.255 B(config-router)# passive-interface default B(config-router)# no passive-interface GigabitEthernet 0/1
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# router rip C(config-router)# version 2 C(config-router)#no auto-summary C(config-router)# network 0.0.0.0 255.255.255.255 C(config-router)# passive-interface default C(config-router)# no passive-interface GigabitEthernet 0/1
Verification	Check the routing tables on Router A, Router B, and Router C. Verify that RIP learns the routes to remote networks (contents marked in blue).
A	A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

	E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1 C 155.10.1.0/24 is directly connected, GigabitEthernet 0/2 C 155.10.1.1/32 is local host. C 192.168.217.0/24 is directly connected, VLAN 1 C 192.168.217.233/32 is local host. R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
B	B# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.2/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1 C 196.38.165.0/24 is directly connected, GigabitEthernet 0/2 C 196.38.165.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C	C# show ip route

```
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.3/32 is local host.
C    117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C    117.102.0.1/32 is local host.
R    155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R    196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version on the device is different from that on other routers.
- The address range configured by the **network** command does not cover a specific interface.
- The **wildcard** parameter in the **network** command is not correctly configured. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
- The interface used for interconnection between devices is configured as a passive interface.

4.4.2 Controlling Interaction of RIP Packets

Configuration Effect

Change the default running mechanism of RIP through configuration and manually control the interaction mode of RIP packets, including:

- Allowing or prohibiting the sending of unicast RIP packets to a specified neighbor on an interface
- Allowing or prohibiting the sending of unicast RIPv2 packets instead of broadcast packets to a specified neighbor on an interface
- Allowing or prohibiting the receiving of RIP packets on an interface
- Allowing or prohibiting the sending of RIP packets on an interface
- Allowing or prohibiting the receiving of RIP packets of a specified version on an interface

- Allowing or prohibiting the sending of RIP packets of a specified version on an interface

Notes

- The RIP basic functions must be configured.
- On an interface connecting to a neighbor device, the configured version of sent RIP packets must be the same as the version of received RIP packets.

Configuration Steps

Sending Unicast RIP Route Update Packets to a Specified Neighbor

- Configure this function if you wish that only some of devices connected to an interface can receive the updated routing information.
- By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise the routing information, whereas RIPv2 uses the multicast address (224.0.0.9) to advertise the routing information. If you do not wish all devices on the broadcast network or NBMA network to receive routing information, configure the related interface as the passive interface and specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. RIPv2 packets are broadcast on an interface.
- Unless otherwise required, this function must be enabled on a router that sends the unicast Update packets.

Broadcasting RIPv2 Packets on an Interface

- This function must be configured if the neighbor router does not support the receiving of multicast RIPv2 packets.
- Unless otherwise required, this function must be configured on every router interface that broadcasts RIPv2 packets.

Allowing an Interface to Receive RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to receive RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to receive RIP packets.

Allowing an Interface to Send RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to send RIP packets.
- Unless otherwise required, this function must be configured on every router interface that is not allowed to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be sent on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to send RIP packets of a specified version.

Allowing an Interface to Receive RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be received on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on every router interface that is allowed to receive RIP packets of a specified version.

Verification

Run the **debug ip rip packet** command to verify the packet sending result and packet type.

Related Commands

Sending Unicast RIP Route Update Packets to a Specified Neighbor

Command Syntax	**neighbor** *ip-address*
Parameter Description	*ip-address:* Indicates the IP address of the neighbor. It should be the address of the network directly connected to the local device.
Command Mode	Routing process configuration mode
Configuration Usage	Generally, you can first run the **passive-interface** command in routing process configuration mode to configure the related interface as a passive interface, and then specify the neighbors that can receive the routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send the request packets even after the device is restarted.

Broadcasting RIPv2 Packets on an Interface

Command Syntax	**ip rip v2-broadcast**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the configuration of the **version** command.

Allowing an Interface to Receive RIP Packets

Command Syntax	**ip rip receive enable**
Parameter Description	N/A

Command Mode	Interface configuration mode
Configuration Usage	To prohibit the receiving of RIP packets on an interface, use the **no** form of this command. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to receive RIP packets.

Allowing an Interface to Send RIP Packets

Command Syntax	**ip rip send enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit the sending of RIP packets on an interface, use the **no** form of this command in interface configuration mode. This command takes effect only on the current interface. You can use the **default** form of the command to restore the default setting, that is, allowing the interface to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

Command Syntax	**ip rip send version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are sent. **2**: Indicates that only RIPv2 packets are sent.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the current interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the configuration of the **version** command.

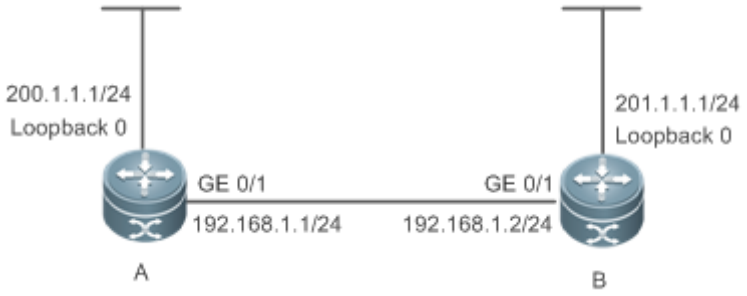
Allowing an Interface to Receive RIP Packets of a Specified Version

Command Syntax	**ip rip receive version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are received. **2**: Indicates that only RIPv2 packets are received.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the configuration of the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of receiving RIP packets on the current interface, and the interface is allowed to receive RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving

	RIP packets is determined by the configuration of the **version** command.

Configuration Example

↘ Prohibiting an Interface from Sending RIP Packets

Scenario **Figure 4-8**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP packets on an interface of Router A.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)# no ip rip send enable`
Verification	Run the **debug ip rip packet send** command on Router A, and verify that packets cannot be sent.
A	`A# debug ip rip packet recv` `*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Prepare to send BROADCAST response...` `*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Building update entries on GigabitEthernet 0/1` `*Nov 4 08:19:31: %RIP-7-DEBUG: 117.0.0.0/8 via 0.0.0.0 metric 1 tag 0` `*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!`

Common Errors

A compatibility error occurs because the RIP version configured on the neighbor is different from that configured on the local device.

4.4.3 Enabling Triggered Updates

Configuration Effect

- Enable the RIP triggered updates function, after which RIP does not periodically send the route update packets.

Notes

- The RIP basic functions must be configured.

- It is recommended that split horizon with poisoned reverse be enabled; otherwise, invalid routing information may exist.
- Ensure that the triggered updates function is enabled on every router on the same link; otherwise, the routing information cannot be exchanged properly.

Configuration Steps

Enabling Triggered Updates

- This function must be enabled if demand circuits are configured on the WAN interface.
- The triggered updates function can be enabled in either of the following cases: (1) The interface has only one neighbor; (2) The interface has multiple neighbors but the device interacts with these neighbors in unicast mode.
- It is recommended that triggered updates be enabled on a WAN interface (running the PPP, Frame Relay, or X.25 link layer protocol) to meet the requirements of demand circuits.
- If the triggered updates function is enabled on an interface, source address verification is performed no matter whether the source address verification function is enabled by the **validate-update-source** command.
- Unless otherwise required, triggered updates must be enabled on demand circuits of every router.

Verification

When the RIP triggered updates function is enabled, RIP cannot periodically send the route update packets. RIP sends the route update packets to the WAN interface only in one of the following cases:

- A route request packet is received.
- The RIP routing information changes.
- The interface state changes.
- The router is started.

Related Commands

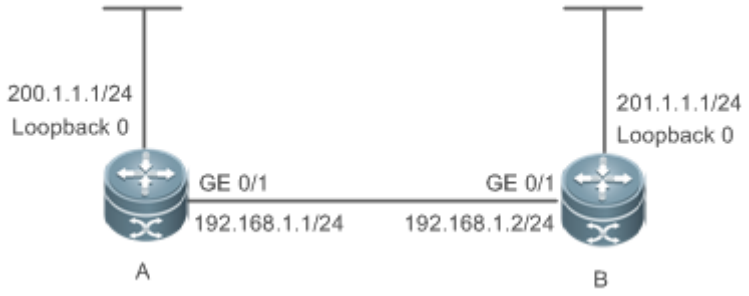
Enabling Triggered Updates

Command Syntax	**ip rip triggered** { **retransmit-timer** *timer* | **retransmit-count** *count* }
Parameter Description	**retransmit-timer** *timer*: Configures the interval at which the update request or update response packet is retransmitted. The default value is 5s. The value ranges from 1 to 3,600. **retransmit-count** *count*: Configures the maximum retransmission times of the update request or update response packet. The default value is 36. The value ranges from 1 to 3,600.
Command Mode	Interface configuration mode
Configuration Usage	You can run the **ip rip triggered** command to enable the RIP triggering function. When this function is enabled, the RIP periodical update function is automatically disabled. Therefore, the acknowledgment and retransmission mechanisms must be used to ensure that the Update packets are successfully sent or received on the WAN. You can use the **retransmit-timer** and **retransmit-count**

	parameters to specify the retransmission interval and maximum retransmission times of the request and update packets.

Configuration Example

Enabling Triggered Updates

Scenario **Figure 4-9**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router A, enable the RIP triggered updates function, and set the retransmission interval and maximum retransmission times of the request and update packets to 10s and 18, respectively.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# encapsulation ppp A(config-if-GigabitEthernet 0/1)# ip rip triggered A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10 A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18 A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse A(config)# router rip A(config-router)# network 192.168.1.0 A(config-router)# network 200.1.1.0
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# encapsulation ppp B(config-if-GigabitEthernet 0/1)# ip rip triggered B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse B(config)# router rip B(config-router)# network 192.168.1.0

	B(config-router)# network 201.1.1.0
Verification	On Router A and Router B, check the RIP database and verify that the corresponding routes are permanent.
A	A# sho ip rip database 201.1.1.0/24 auto-summary 201.1.1.0/24 [1] via 192.168.12.2 GigabitEthernet 0/1 06:25 permanent
B	B# sho ip rip database 200.1.1.0/24 auto-summary 200.1.1.0/24 [1] via 192.168.12.1 GigabitEthernet 0/1 06:25 permanent

Common Errors

- The triggered updates function is enabled when the RIP configurations at both ends of the link are consistent.
- The triggered updates function is not enabled on all routers on the same link.

4.4.4 Enabling Source Address Verification

Configuration Effect

- The source address of the received RIP route update packet is verified.

Notes

- The RIP basic functions must be configured.

Configuration Steps

↘ Enabling Source Address Verification

- This function is enabled by default, and must be disabled when source address verification is not required.
- After split horizon is disabled on an interface, the RIP routing process will perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- For an IP unnumbered interface, the RIP routing process does not perform source address verification on the Update packet no matter whether the **validate-update-source** command is executed in routing process configuration mode.
- Unless otherwise required, this function must be disabled on every router that does not requires source address verification.

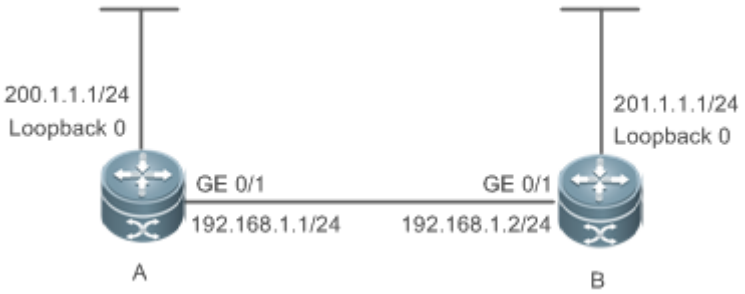
Verification

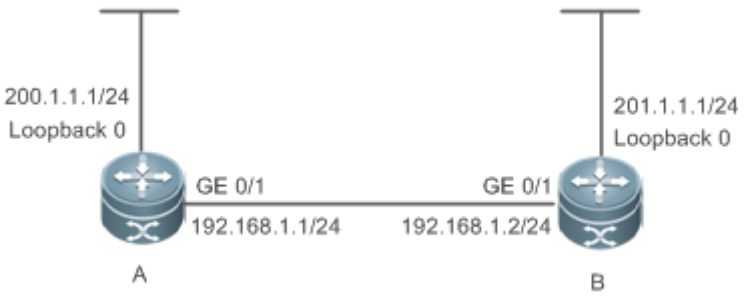
Only the route update packets coming from the same IP subnet neighbor are received.

Related Commands

Command Syntax	**validate-update-source**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Source address verification of the Update packet is enabled by default. After this function is enabled, the source address of the RIP route update packet is verified. The purpose is to ensure that the RIP routing process receives only the route update packets coming from the same IP subnet neighbor.

Configuration Example

Scenario Figure 4-10	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Disable source address verification of Update packets on all routers.
A	`A# configure terminal` `A(config)# router rip` `A(config-router)# no validate-update-source`
B	`B# configure terminal` `B(config)# router rip` `B(config-router)# no validate-update-source`
Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	`A# show ip route rip` `R  201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1`
B	`B# show ip route rip`

Scenario **Figure 4-10**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Disable source address verification of Update packets on all routers.
A	`A# configure terminal` `A(config)# router rip` `A(config-router)# no validate-update-source`
B	`B# configure terminal` `B(config)# router rip` `B(config-router)# no validate-update-source`
Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
	`R  200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1`

4.4.5 Enabling Authentication

Configuration Effect

- Prevent learning unauthenticated and invalid routes and advertising valid routes to unauthorized devices, ensuring stability of the system and protecting the system against intrusions.

Notes

- The RIP basic functions must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Configuration Steps

↘ Enabling Authentication and Specifying the Key Chain Used for RIP Authentication

- This configuration is mandatory if authentication must be enabled.
- If the key chain is already specified in the interface configuration, run the **key chain** command in global configuration mode to define the key chain; otherwise, authentication of RIP packets may fail.

- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Defining the RIP Authentication Mode

- This configuration is mandatory if authentication must be enabled.
- The RIP authentication modes configured on all devices that need to directly exchange RIP routing information must be the same; otherwise, RIP packets may fail to be exchanged.
- If plain text authentication is used, but the key chain for plain text authentication is not configured or associated, authentication is not performed. Similarly, if MD5 authentication is used, but the key chain is not configured or associated, authentication is not performed.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Enabling RIP Plain Text Authentication and Configuring the Key Chain

- This configuration is mandatory if authentication must be enabled.
- If RIP plain text authentication should be enabled, use this command to configure the key chain for plain text authentication. Alternatively, you can obtain the key chain for plain text authentication by associating the key chain. The key chain obtained using the second method takes precedence over that obtained using the first method.
- Unless otherwise required, this configuration must be performed on every router that requires authentication.

Verification

- RIP plain text authentication provides only limited security because the password transferred through the packet is visible.
- RIP MD5 authentication can provide higher security because the password transferred through the packet is encrypted using the MD5 algorithm.
- Routes can be learned properly if the correct authentication parameters are configured.
- Routes cannot be learned if the incorrect authentication parameters are configured.

Related Commands

Enabling Source Address Verification

Command Syntax	**ip rip authentication key-chain** *name-of-keychain*
Parameter Description	*name-of-keychain*: Specifies the name of the key chain used for RIP authentication.
Command Mode	Interface configuration mode
Configuration Usage	The specified key chain must be defined by the **key chain** command in global configuration mode in advance.

Defining the RIP Authentication Mode

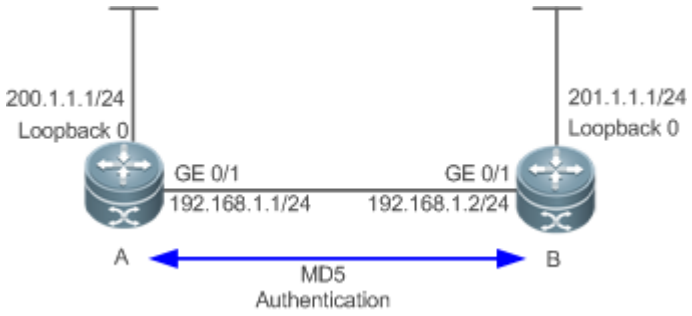
Command Syntax	**ip rip authentication mode** { **text** | **md5** }
Parameter Description	**text:** Indicates that the RIP authentication mode is plain text authentication. **md5:** Indicates that the RIP authentication mode is MD5 authentication.
Command Mode	Interface configuration mode
Configuration Usage	For all devices that need to directly exchange the RIP routing information, the RIP authentication mode of these devices must be the same.

Enabling RIP Plain Text Authentication and Configuring the Key Chain

Command Syntax	**ip rip authentication text-password** [**0** | **7**] *password-string*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *password-string*: Indicates the key chain used for plain text authentication. The key chain is a string of 1 to 16 bytes.
Command Mode	Interface configuration mode
Configuration Usage	This commands takes effect only in plain text authentication mode.

Configuration Example

Configuring RIP Basic Functions and Enabling MD5 Authentication

Scenario Figure 4-11	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.
A	`A# configure terminal` `A(config)# key chain hello` `A(config-keychain)# key 1` `A(config-keychain-key)# key-string world`

	A(config-keychain-key)# exit A(config-keychain)# exit A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
B	B# configure terminal B(config)# key chain hello B(config-keychain)# key 1 B(config-keychain-key)# key-string world B(config-keychain-key)# exit B(config-keychain)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
Verification	• On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. • On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

Common Errors

- The keys configured on routers that need to exchange RIP routing information are different.
- The authentication modes configured on routers that need to exchange RIP routing information are different.

4.4.6 Enabling Route Summarization

Configuration Effect

Reduce the size of the routing table, improve the routing efficiency, avoid route flapping to some extent, and improve scalability and effectiveness of the network.

If a summarized route exists, subroutes included by the summarized route cannot be seen in the routing table, which greatly reduces the size of the routing table.

Advertising a summarized route is more efficient than advertising individual routes because: (1) A summarized route is processed first when RIP looks through the database; (2) All subroutes are ignored when RIP looks through the database, which reduces the processing time required.

Notes

- The RIP basic functions must be configured.
- The range of supernetting routes is larger than that of the classful network. Therefore, the automatic route summarization function is invalid for supernetting routes.
- RIPv1 always performs automatic route summarization. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

Configuration Steps

Enabling Automatic Route Summarization

- This function is enabled by default.
- To learn specific subnet routes instead of summarized network routes, you must disable automatic route summarization.
- You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

- This function must be configured if it is required to summarize classful subnets.
- The **ip rip summary-address** command is used to summarize an address or a subnet under a specified interface. RIP automatically summarizes to the classful network boundary. Each classful subnet can be configured only in the **ip rip summary-address** command.
- The summary range configured in this command cannot be supernetting routes, that is, the configured subnet mask length cannot be smaller than the natural mask length of the network.
- Unless otherwise required, this configuration should be performed on a router that requires classful subnet summarization.

Verification

Verify that the routes are summarized in the routing table of the peer end.

Related Commands

Enabling Automatic Route Summarization

Command Syntax	**auto-summary**
Parameter Description	N/A

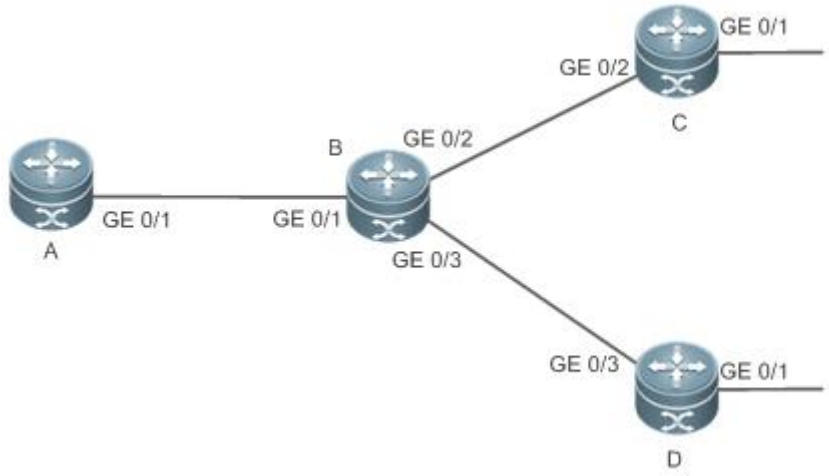
Command Mode	Routing process configuration mode
Configuration Usage	Route summarization is enabled by default for RIPv1 and RIPv2. You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

Command Syntax	**ip rip summary-address** *ip-address ip-network-mask*
Parameter Description	*ip-address*: Indicates the IP address to be summarized. *ip-network-mask*: Indicates the subnet mask of the IP address to be summarized.
Command Mode	Interface configuration mode
Configuration Usage	This command is used to summarize an address or a subnet under a specified interface.

Configuration Example

Configuring Route Summarization

Scenario **Figure 4-12**	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure route summarization on Router B.

	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0 B(config)# router rip B(config-router)# version 2 B(config-router)# no auto-summary
Verification	Check the routing table on Router A, and verify that the entry 172.16.0.0/16 is generated.
	A# show ip route rip R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1

Common Errors

- RIP basic functions are not configured or fail to be configured.

4.4.7 Enabling Supernetting Routes

Configuration Effect

- Allow RIP to send RIP supernetting routes on a specified interface.

Notes

- The RIP basic functions must be configured.

Configuration Steps

↘ Enabling Supernetting Routes

- If a supernetting route is detected when a RIPv1-enabled router monitors the RIPv2 route response packets, the router will learn an incorrect route because RIPv1 ignores the subnet mask in the routing information of the packet. In this case, the **no** form of the command must be used on the RIPv2-enabled router to prohibit advertisement of supernetting routes on the related interface. This command takes effect only on the current interface.
- The command is effective only when RIPv2 packets are sent on the interface, and is used to control the sending of supernetting routes.

Verification

Verify that the peer router cannot learn the supernetting route.

Related Commands

Command Syntax	**ip rip send supernet-routes**

Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	By default, an interface is allowed to send RIP supernetting routes.

Configuration Example

Disabling Supernetting Routes

Scenario **Figure 4-13**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Prohibit the sending of RIP supernetting routes on the GigabitEthernet 0/1 interface of Router B.
	B# configure terminal B(config)# ip route 207.0.0.0 255.0.0.0 Null 0 B(config)# ip route 208.1.1.0 255.255.255.0 Null 0 B(config)# router rip B(config-router)# redistribute static B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes
Verification	Check the routing table on Router A, and verify that Router A can learn only the non-supernetting route 208.1.1.0/24, but not the supernetting route 207.0.0.0/8.
	A#show ip route rip R 208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

4.4.8 Advertising the Default Route or External Routes

Configuration Effect

- In the RIP domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

- In the RIP domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

Notes

- The RIP basic functions must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

Configuration Steps

Advertising the Default Route to Neighbors

This function must be enabled if it is required to advertise the default route to neighbors.

By default, a default route is not generated, and the metric of the default route is 1.

If the RIP process can generate a default route using this command, RIP does not learn the default route advertised by the neighbor.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Advertising the Default Route to Neighbors on an Interface

This function must be enabled if it is required to advertise the default route to neighbors on a specified interface.

By default, a default route is not configured and the metric of the default route is 1.

After this command is configured on an interface, a default route is generated and advertised through this interface.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

Redistributes Routes and Advertises External Routes to Neighbors

This function must be enabled if routes of other protocols need to be redistributed.

By default,

- If OSPF redistribution is configured, redistribute the routes of all sub-types of the OSPF process.
- In other cases, redistribute all external routes.
- The metric of a redistributed route is 1 by default.
- The route map is not associated by default.

During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, however, it is necessary to configure a symbolic metric; otherwise, route redistribution fails.

Unless otherwise required, this configuration should be performed on a router that needs to redistribute routes.

Verification

- On a neighbor device, verify that a default route exists in the RIP routing table.
- On the local and neighbor devices, verify that external routes (routes to other ASs) exist in the RIP routing table.

Related Commands

Advertising the Default Route to Neighbors

Command Syntax	**default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]
Parameter Description	**always:** Enables RIP to generate a default route no matter whether the local router has a default route. **metric** *metric-value:* Indicates the initial metric of the default route. The value ranges from 1 to 15. **route-map** *map-name:* Indicates the associated route map name. By default, no route map is associated.
Command Mode	Routing process configuration mode
Configuration Usage	If a default route exists in the routing table of a router, RIP does not advertise the default route to external entities by default. You need to run the **default-information originate** command in routing process configuration mode to advertise the default route to neighbors. If the **always** parameter is selected, the RIP routing process advertises a default route to neighbors no matter the default route exists, but this default route is not displayed in the local routing table. To check whether the default route is generated, run the **show ip rip database** command to check the RIP routing information database. To further control the behavior of advertising the RIP default route, use the **route-map** parameter. For example, run the **set metric** rule to set the metric of the default route. You can use the **metric** parameter to set the metric of the advertised default value, but the priority of this configuration is lower than that of the set metric rule of the **route-map** parameter. If the **metric** parameter is not configured, the default route uses the default metric configured for RIP. You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

Advertising the Default Route to Neighbors on an Interface

Command Syntax	**ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]
Parameter Description	**only**: Indicates that only the default route is advertised. **originate**: Indicates that the default route and other routes are advertised. **metric** *metric-value:* Indicates the metric of the default route. The value ranges from 1 to 15.
Command Mode	Interface configuration mode
Configuration Usage	If you configure the **ip rip default-information** command for the interface, and the **default-information originate** command for the RIP process, only the default route configured for the interface is advertised. So far as **ip rip default-information** is configured for one interface, RIP does not learn the default route advertised by the neighbor.

Redistributes Routes and Advertises External Routes to Neighbors

Command Syntax	**redistribute** { **connected** |**ospf** *process-id* | **static** } [**match** { **internal | external** [**1 | 2**] **| nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]
Parameter Description	**connected**: Indicates redistribution from direct routes. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value ranges from 1 to 65535. **static**: Indicates redistribution from static routes. **match**: Used only when OSPF routes are redistributed. Only the routes that match the filtering conditions are redistributed. **metric** *metric-value*: Sets the metric of the redistributed route. The value ranges from 1 to 16. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode
Configuration Usage	If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Configuration Example

Redistributing Routes and Advertising External Routes to Neighbors

Scenario Figure 4-14	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router B, configure redistribution of static routes.
B	`B# configure terminal` `B(config)# router rip` `B(config-router)# redistribute static`
Verification	On Router A, check the routing table and verify that the entry 172.10.10.0/24 is loaded.

	A# show ip route rip R 172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

4.4.9 Setting Route Filtering Rules

Configuration Effect

- Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

Notes

- The RIP basic functions must be configured.
- In regard to the filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

Configuration Steps

↘ Filtering the Received RIP Routing Information

- This function must be configured if it is required to filter received routing information.
- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

↘ Filtering the Sent RIP Routing Information

- This function must be configured if it is required to filter the redistributed routing information that is sent.
- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route rip** command to verify that the routes that have been filtered out are not loaded to the routing table.

Related Commands

↘ Filtering the Received RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

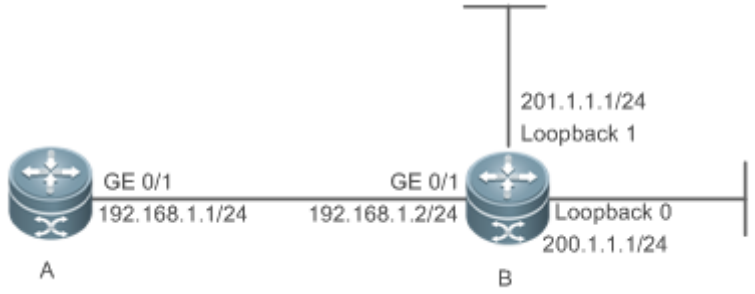
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be received. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. **gateway** *prefix-list-name*: Uses the prefix list to filter the route sources. *interface-type interface-number*: Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

Filtering the Sent RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected| ospf** *process-id* **| rip | static**]]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be sent. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. *Interface*: Applies route update advertisement control only on the specified interface. **connected**: Applies route update advertisement control only on direct routes introduced through redistribution. **ospf** *process-id*: Applies route update advertisement control only on the routes introduced from OSPF. *process-id* specifies an OSPF process. **rip**: Applies route update advertisement control only on RIP routes. **static**: Applies route update advertisement control only on static routes introduced through redistribution.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

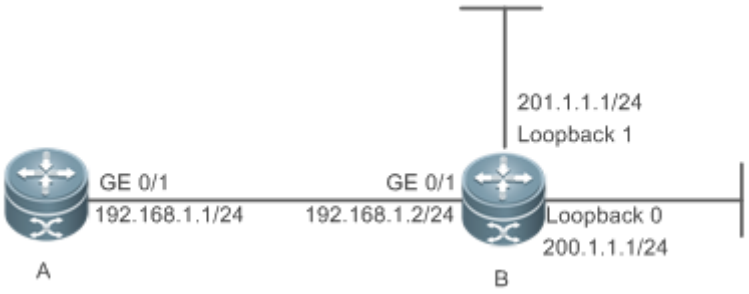
Configuration Example

Filtering the Received RIP Routing Information

Scenario **Figure 4-15**	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to control routes received over the GigabitEthernet 0/1 port and receive only the route 200.1.1.0.
A	A# configure terminal A(config)# router rip A(config-router)# distribute-list 10 in GigabitEthernet 0/1 A(config-router)# no auto-summary A(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Verification	On Router A, check the routing table and verify that only the entry 200.1.1.0/24 exists.
A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Filtering the Sent RIP Routing Information

Scenario **Figure 4-16**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Enable the RIP routing process to advertise only the route 200.1.1.0/24.
B	B# configure terminal B(config)# router rip B(config-router)# redistribute connected B(config-router)# distribute-list 10 out B(config-router)# version 2 B(config)# access-list 10 permit 200.1.1.0 0.0.0.255
Verification	Check the routing table on Router A, and verify that route in the 200.1.1.0 network segment exists.

A	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1

Common Errors

- Filtering fails because the filtering rules of the access list are not properly configured.

4.4.10 Modifying Route Selection Parameters

Configuration Effect

- Change the RIP routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects various types of routes so as to change the priorities of RIP routes.

Notes

- The RIP basic functions must be configured.

Configuration Steps

Modifying the Administrative Distance of a RIP Route

- Optional.
- This configuration is mandatory if you wish to change the priorities of RIP routes on a router that runs multiple unicast routing protocols.

Increasing the Metric of a Received or Sent RIP Route

- Optional.
- Unless otherwise required, this configuration should be performed on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIP

- Optional.
- Unless otherwise required, this configuration must be performed on an ASBR to which external routes are introduced.

Verification

Run the **show ip rip** command to display the administrative distance currently configured. Run the **show ip rip data** command to display the metrics of redistributed routes to verify that the configuration takes effect.

Related Commands

Modifying the Administrative Distance of a RIP Route

Command	**distance** *distance* [*ip-address wildcard*]

Syntax	
Parameter Description	*distance*: Sets the administrative distance of a RIP route. The value is an integer ranging from 1 to 255. *ip-address*: Indicates the prefix of the source IP address of the route. *wildcard*: Defines the IP address comparison bit. **0** indicates accurate matching, and **1** indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to configure the administrative distance of a RIP route.

Increasing the Metric of a Received or Sent RIP Route

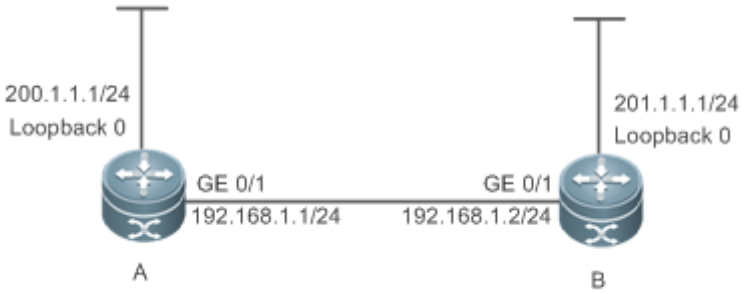
Command Syntax	**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. **In**: Uses the ACL to modify the metric of a received route. **out**: Uses the ACL to modify the metric of a sent route. *offset*: Indicates the offset of the modified metric. The value ranges from 0 to 16. *interface-type*: Uses the ACL on the specified interface. *interface-number*: Specifies the interface number.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to increase the metric of a received or sent RIP route. If the interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

Configuring the Default Metric of an External Route Redistributed to RIP

Command Syntax	**default-metric** *metric-value*
Parameter Description	*metric-value:* Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the RGOS determines that this route is unreachable.
Command Mode	Routing process configuration mode
Configuration Usage	This command must be used together with the routing protocol configuration command **redistribute**.

Configuration Example

Increasing the Metric of a Received or Sent RIP Route

Scenario **Figure 4-17**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Increase by 7 the metric of each RIP route in the range specified by ACL 7. ● Increase by 7 the metric of each learned RIP route in the range specified by ACL 8.
A	`A# configure terminal` `A(config)# access-list 7 permit host 200.1.1.0` `A(config)# access-list 8 permit host 201.1.1.0` `A(config)# router rip` `A(config-router)# offset-list 7 out 7` `A(config-router)# offset-list 8 in 7`
Verification	Check the routing table on Router A and Router B to verify that the metrics of RIP routes are 8.
A	`A# show ip route rip` `R    201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`
B	`B# show ip route rip` `R    200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1`

4.4.11 Modifying Timers

Configuration Effect

- Change the duration of RIP timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- The RIP basic functions must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

Configuration Steps

Modifying the Update Timer, Invalid Timer, and Flush Timer

This configuration must be performed if you need to adjust the RIP timers.

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For routers connected to the same network, values of the three RIP timers must be the same. Generally, you are advised not to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of Update packets consume the bandwidth. You can set timers to small values generally on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

Unless otherwise required, this configuration should be performed on a router where RIP timers need to be modified.

Setting the Sending Delay Between RIP Route Update Packets

This configuration must be performed if you need to adjust the sending delay between RIP Update packets.

Run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all Update packets.

Unless otherwise required, this configuration should be performed on a router where the sending delay needs to be adjusted.

Verification

Run the **show ip rip** command to display the current settings of RIP timers.

Related Commands

Modifying the Update Timer, Invalid Timer, and Flush Timer

Command Syntax	**timers basic** *update invalid flush*
Parameter Description	*update*: Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an Update packet is received, the invalid timer and flush timer are reset. By default, a routing update packet is sent every 30s. *invalid*: Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no Update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the Update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *flush*: Indicates the route flushing time in second, counted from the time when the RIP route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Configuration	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

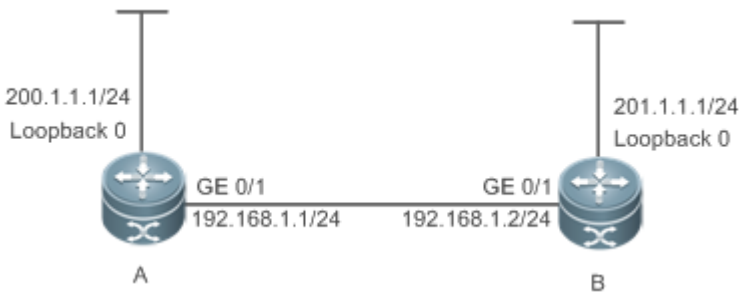
Usage	

Setting the Sending Delay Between RIP Route Update Packets

Command Syntax	**output-delay** *delay*
Parameter Description	*delay:* Sets the sending delay between packets in ms. The value ranges from 8 to 50.
Command Mode	Interface configuration mode
Configuration Usage	Normally, a RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible. When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may not be able to process all update packets in time, causing a loss of routing information. In this case, you need to run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Configuration Example

Setting the Sending Delay Between RIP Route Update Packets

Scenario Figure 4-18	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● Configure the sending delay of update packets on Router A.
A	`A# configure terminal` `A(config)# router rip` `A(config-router)# output-delay 30`
Verification	Capture packets on Router A and compare the sending time of update packets before and after the configuration, and verify that a delay of 30 ms is introduced.

Common Errors

For routers connected to the same network, values of the three RIP timers are not the same.

4.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active board to the standby board, traffic forwarding continues and is not interrupted.
- When the RIP process is being restarted, traffic forwarding continues and is not interrupted.

Notes

- The RIP basic functions must be configured.
- The GR period is at least twice the RIP route update period.
- During the RIP GR process, ensure that the network environment is stable.

Configuration Steps

↘ Configuring the GR Restarter Capability

This configuration must be performed if RIP needs to be gracefully restarted to ensure data forwarding during hot standby switchover.

The GR function is configured based on the RIP process. You can configure different parameters for different RIP processes based on the actual conditions.

The GR period is the maximum time from restart of the RIP process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIP route is restored so as to restore the RIP state before the restart. After the restart period expires, RIP exits from the GR state and performs common RIP operations.

Unless otherwise required, this configuration should be performed on every router that needs to be gracefully restarted.

Verification

- Run the **show ip rip** command to display the GR state and configured time.
- Trigger a hot standby switchover, and verify that data forwarding is not interrupted.

Related Commands

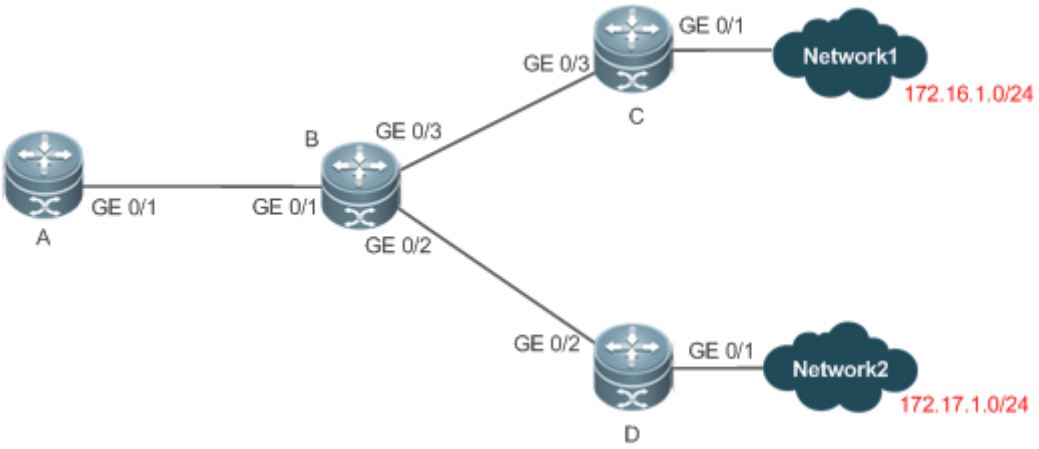
↘ Configuring the GR Restarter Capability

Command Syntax	**graceful-restart** [**grace-period** *grace-period*]
Parameter Description	**graceful-restart**: Enables the GR function. **grace-period**: Explicitly configures the grace period. *grace-period*: Indicates the GR period. The value ranges from 1s to 1800s. The default value is twice the update time or 60s, whichever is the smaller.
Command Mode	Routing process configuration mode

Configuration Usage	This command allows you to explicitly modify the GR period. Note that GR must be completed after the update timer of the RIP route expires and before the invalid timer of the RIP route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are advised not to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalid timer based on the configuration of the **timers basic** command.

Configuration Example

↘ Configuring the GR Restarter Capability

Scenario **Figure 4-19**	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the RIP basic functions on all routers. (Omitted) ● On Router B, enable the GR function.
	`B# configure terminal` `B(config)# router rip` `B(config-router)# graceful-restart grace-period 90`
Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

4.5 Monitoring

Displaying

Description	Command
Displays the basic information about a RIP process.	**show ip rip**
Displays the RIP routing table.	**show ip rip database** [*network-number network-mask*] [**count**]
Displays information about external routes redistributed by RIP.	**show ip rip external** [**connected** | **ospf** *process-id* | **static**]
Displays the RIP interface information.	**show ip rip interface** [*interface-type interface-number*]
Displays the RIP neighbor information.	**show ip rip peer** [*ip-address*]

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs events that occur when the RIP process is running.	**debug ip rip event**
Debugs interaction with the NSM process.	**debug ip rip nsm**
Debugs the sent and received packets.	**debug ip rip packet** [**interface** *interface-type interface-number* | **recv** | **send**]
Debugs the RIP GR process.	**debug ip rip restart**
Debugs the route changes of the RIP process.	**debug ip rip route**

5 Configuring RIPng

5.1 Overview

RIP next generation (RIPng) is a unicast routing protocol that applies to IPv6 networks. RIPng-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIPng can run only within the autonomous system (AS) and is applicable to small-sized networks with routes no more than 16 hops.

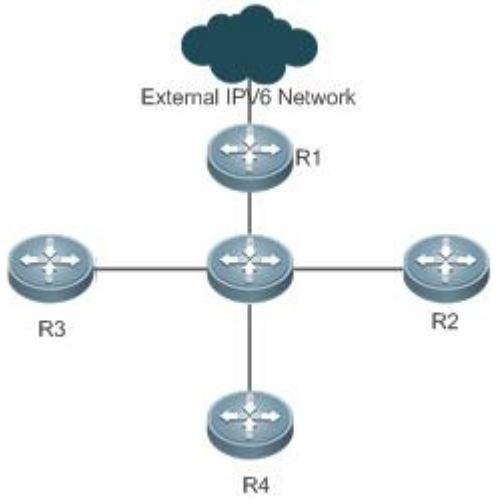
Protocols and Standards

- RFC2080: Defines the RIPng.

5.2 Application

RIPng is generally used on some small-sized networks, such as office networks of small companies.

As shown in the following figure, the company builds an IPv6 network, on which all routers support IPv6. The network is small in size, but the workload is still heavy if the network is maintained manually. In this case, RIPng can be configured to adapt to topological changes of the small-sized network, which reduces the workload.



5.3 Features

Basic Concepts

IGP and EGP

IGP runs within an AS. For example, RIPng is a type of IGP.

Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is a type of EGP.

Feature

Feature	Description
RIPng and RIP	RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.
Exchanging Routing Information	By exchanging routing information, RIPng-enabled devices can automatically obtain routes to a remote network and update routes in real time.
Routing Algorithm	RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.
Avoiding Route Loops	RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

5.3.1 RIPng and RIP

RIP applies to IPv4 networks. Two RIP versions are available, including RIPv1 and RIPv2.

RIPng is an extension of RIPv2 on the basis of IPv6. Both are similar in functions and configurations.

Working Principle

RIPv2

RIPv2 packets are multicast. The multicast address is 224.0.0.9, and the UDP port ID is 520. RIPv2 can identify the subnet mask.

RIPng

RIPng packets are multicast. The multicast address is FF02::9, the source address is FE80::/10, and the UDP port ID is 521. RIPng can identify the subnet mask.

This chapter describes functions and configurations of RIPng. For details about RIPv2, see "Configuring RIP".

Related Configuration

Enabling the RIPng Process

By default, the RIPng process is disabled.

Run the **ipv6 router rip** command to enable the RIPng process.

You must enable the RIPng process on a device; otherwise, all functions related to RIPng cannot take effect.

Running RIPng on an Interface

By default, RIPng does not run on an interface.

Run the **ipv6 rip enable** command to run RIPng on an interface.

After RIPng runs on an interface, RIPng packets can be exchanged on the interface and RIPng can learn routes to the network segments directly connected to the device.

Prohibiting an Interface from Sending or Receiving Packets

By default, a RIPng-enabled interface is allowed to send and receive RIPng packets.
Run the **passive-interface** command to prohibit an interface from sending RIPng packets.

5.3.2 Exchanging Routing Information

Compared with static routing, the dynamic routing protocol has a significant advantage, that is, by exchanging routing information, devices can automatically obtain routes to a remote network and update the routes in real time.

Working Principle

Initialization

After RIPng is enabled on a router, the router sends a request packet to its neighbor router, requesting for all routing information, that is, the routing table. After receiving the request message, the neighbor router returns a response packet containing the local routing table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighbor router, informing the neighbor router of the route update information. After receiving the update packet, the neighbor router updates the local routing table, and sends the update packet to other adjacent routers. After a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIPng. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighbor routers.

For every non-local route, if the route is not updated within 180s (invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (flush timer), the route is deleted from the routing table.

Default Route

In the routing table, a route to the destination network ::/0 is called default route.
The default route can be learned from a neighbor router, or sent to a neighbor router.

Route Redistribution

For RIPng, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.
External routes (excluding the default route) can be redistributed to RIPng and advertised to neighbors.

Route Filtering

Filtering conditions can be configured to limit the routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

Related Configuration

RIPng Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.
Run the **timers basic** command to modify durations of RIPng timers.

Increasing the duration of the flush timer can reduce the route flapping. Decreasing the duration of the flush timer helps accelerate route convergence.
The durations of RIPng timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to modify the RIPng timers.

Default Route

Run the **ipv6 rip default-information** command to advertise the default route to neighbors on an interface.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIPng and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit the routing information sent by the device.
Run the **distribute-list in** command to set filtering rules to limit the routing information received by the device.

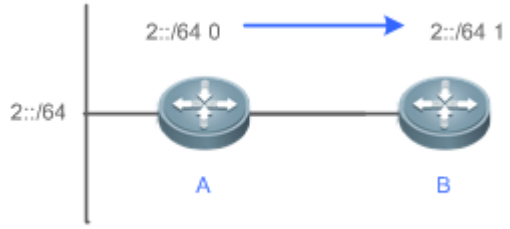
5.3.3 Routing Algorithm

RIPng is a protocol based on the distance-vector algorithm. It uses the vector addition method to compute the routing information.

Working Principle

Distance-Vector Algorithm

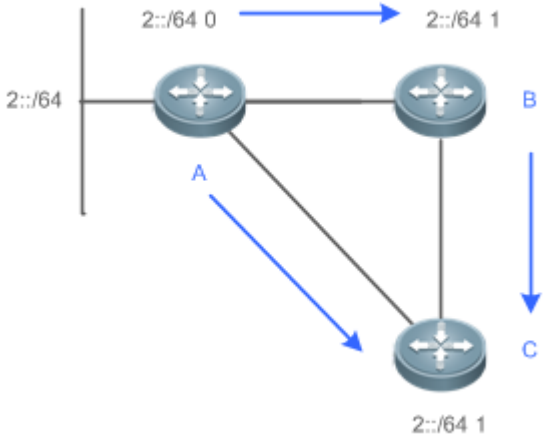
RIPng is a protocol based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance (metric). The router obtains a route from its neighbor and adds the distance vector from itself to the neighbor to the route to form its own route.
RIPng uses the hop count to evaluate the distance (metric) to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through a router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIPng stipulates that the metric must be an integer between 0 and 15. If the metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIPng cannot be applied to a large-scale network.
As shown in the following figure, Router A is connected to the network 2::/64. Router B obtains the route (2::/64, 0) from Router A and adds the metric 1 to the route to obtain its own route (2::/64, 1), and the next hop points to Router A.



Selecting the Optimum Route

RIPng selects an optimum route based on the following principle: If multiple routes to the same destination network is available, a router preferentially selects the route with the smallest metric.

As shown in the following figure, Router A is connected to the network 2::/64. Router C obtains the route (2::/64, 0) from Router A and the route (2::/64, 1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (2::/64, 1), and the next hop points to Router A.



When routes coming from different sources exist on a router, the route with the smaller distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
IS-IS route	115
RIPng route	120
Unreachable route	255

Related Configuration

Modifying the Distance

By default, the distance of a RIPng route is 120.

Run the **distance** command to modify the distance of a RIPng route.

Modifying the Metric

For a RIPng route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. The metric offset of the interface is 1.

For a RIPng router that is manually configured (default route or redistributed route), the default metric is 1.

Run the **ipv6 rip metric-offset** command to modify the metric offset of the interface.

Run the **default-metric** command to modify the default metric of an external route (redistributed route).

Run the **redistribute** command to modify the metric of an external route (redistributed route) when advertising this route.

Run the **ipv6 rip default-information** command to modify the metric of a default route when advertising the default route.

5.3.4 Avoiding Route Loops

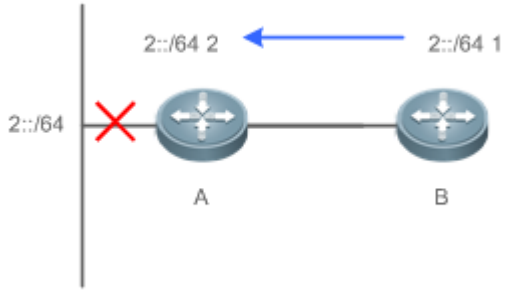
RIPng uses functions, such as split horizon and poison reverse, to avoid route loops.

Working Principle

Route Loop

A RIPng route loop occurs due to inherent defects of the distance-vector algorithm.

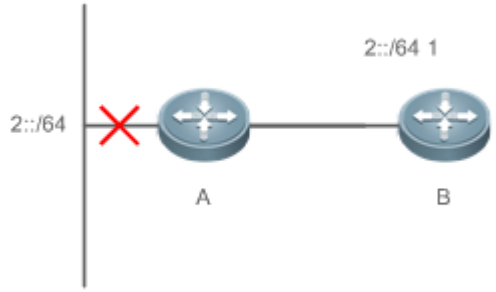
As shown in the following figure, Router A is connected to the network 2::/64, and sends an update packet every 30s. Router B receives the route to 2::/64 from Router A every 30s. If Router A is disconnected from 2::/64, the route to 2::/64 will be deleted from the routing table on Router A. Next time, the update packet sent by Router A no longer contains this route. As Router B does not receive an update packet related to 2::/64, Router B determines that the route to 2::/64 is valid within 180s and uses the update packet to send this route to Router A. As the route to 2::/64 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 2::/64 through Router A, and Router A determines that data can reach 2::/64 through Router B. In this way, a route loop is formed.



Split Horizon

Split horizon can prevent route loops. After split horizon is enabled, a route received on this interface will not be sent out from this interface.

As shown in the following figure, after split horizon is enabled on Router B, Router B will not send the route to 2::/64 back to Router A. Router B will learn 180s later that 2::/64 is not reachable.

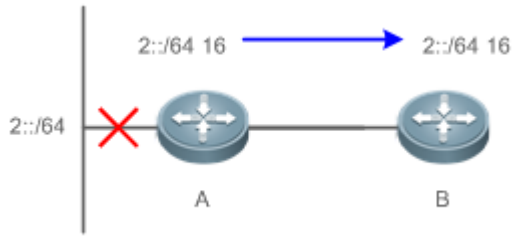


Poison Reverse

Poison reverse can also prevent route loops. Compared with slit horizon, poison reverse is more reliable, but brings more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in the following figure, after poison reverse is enabled on Router A, if Route A detects a disconnection from 2::/64, Router A will not delete the route to 2::/64. Instead, Router A changes the number of hops to 16, and advertises the route through the update packet. On receiving the update packet, Router B learns that 2::/64 is not reachable.



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **split-horizon poisoned-reverse** command to enable poison reverse. (After poison reverse is enabled, split horizon is automatically disabled.)

5.4 Configuration

Configuration	Related Commands	
Configuring RIPng Basic Functions	(Mandatory) It is used to build a RIPng routing domain.	
	ipv6 router rip	Enables a RIPng routing process and enters routing process configuration mode.
	ipv6 rip enable	Runs RIPng on an interface.
	split-horizon	Enables split horizon or poison reverse.
	passive-interface	Configures a passive interface.
Advertising the Default Route or External Routes	(Optional)	
	ipv6 rip default-information	Advertise the default route to neighbors on an interface.
	redistribute	Redistributes routes and advertising external

Configuration	Related Commands	
		routes to neighbors.
Setting Route Filtering Rules	(Optional)	
	distribute-list in	Filters the received RIPng routing information.
	distribute-list out	Filters the sent RIPng routing information.
Modifying Route Selection Parameters	(Optional)	
	distance	Modifies the administrative distance of a RIPng route.
	ipv6 rip metric-offset	Modifies the metric offset on an interface.
	default-metric	Configure the default metric for route redistribution.
Modifying Timers	(Optional)	
	timers	Modifies the update timer, invalid timer, and flush timer of RIPng.
Enabling Authentication and Encryption	(Optional)	
	authentication	Enables authentication on the process.
	encryption	Enables encryption on the process.
	ipv6 rip authentication	Enables authentication on the interface.
	ipv6 rip encryption	Enables encryption on the interface.

5.4.1 Configuring RIPng Basic Functions

Configuration Effect

- Build a RIPng routing domain on the network.
- Routers in the domain obtain routes to a remote network through RIPng.

Notes

- IPv6 addresses must be configured.
- IPv6 unicast routes must be enabled.

Configuration Steps

Enabling a RIPng Routing Process

- Mandatory.
- Unless otherwise required, perform this configuration on every router in the RIPng routing domain.

Running RIPng on an Interface

- Mandatory.
- Unless otherwise required, perform this configuration on every interconnected interface of routers in the RIPng routing domain.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on every interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on every interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access network, such as FR and X.25; otherwise, some devices cannot learn the complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- This configuration is recommended.
- Use the passive interface to set the boundary of the RIPng routing domain. The network segment of the passive interface belongs to the RIPng routing domain, but RIPng packets cannot be sent over the passive interface.
- If RIPng routes need to be exchanged on an interface (such as the router interconnect interface) in the RIPng routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIPng.

Related Commands

Enabling a RIPng Routing Process

Command	**ipv6 router rip**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to create a RIPng routing process and enter routing process configuration mode.

Running RIPng on an Interface

Command	**ipv6 rip enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The configuration for running the RIPng on an interface is different from that of RIPv2. In RIPv2, the **network** command is configured in routing process configuration mode to define an IP address range. If the IP address of an interface belongs to this IP address range, RIP automatically runs on this interface.

Enabling Split Horizon

Command	**split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates that the split horizon function contains the poison reverse function.
Command Mode	Routing process configuration mode
Usage Guide	Run the **show ipv6 rip** command to check whether split horizon is enabled. The configuration is different from that of RIPv2. In RIPv2, the split horizon function is configured in interface configuration mode.

Configuring a Passive Interface

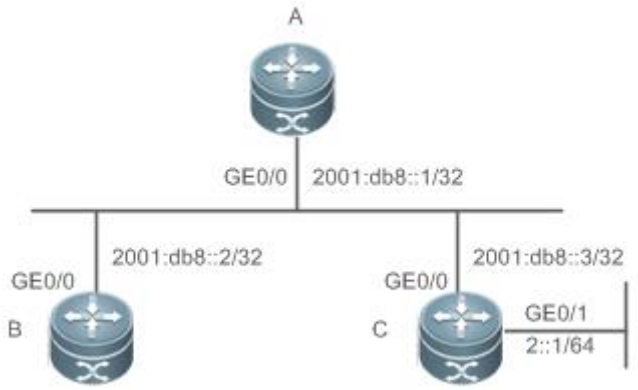
Command	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default:** Indicates all interfaces. ***interface-type interface-num*:** Specifies an interface.
Command Mode	Routing process configuration mode
Usage Guide	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command so that the interfaces used for interconnection between routers in the domain are not passive interface.

Displaying the IP Routing Table

Command	**show ipv6 route**
Parameter Description	N/A
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	Check whether the routing table contains any route to a remote network that is learned through RIPng.

Configuration Example

Building a RIPng Routing Domain

Scenario **Figure 5-1**	
Configuration Steps	● Configure IPv6 addresses on all routers. ● Enable RIPng on all routers.
A	A# configure terminal Enter configuration commands, one per line. End with CNTL/Z. A(config)# ipv6 router rip A(config-router)# exit A(config)# interface GigabitEthernet 0/0 A(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::1/32 A(config-if-GigabitEthernet 0/0)# ipv6 rip enable
B	B# configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)# ipv6 router rip B(config-router)# exit B(config)# interface GigabitEthernet 0/0 B(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::2/32 B(config-if-GigabitEthernet 0/0)# ipv6 rip enable
C	C# configure terminal Enter configuration commands, one per line. End with CNTL/Z. C(config)# ipv6 router rip C(config-router)# exit C(config)# interface GigabitEthernet 0/0 C(config-if-GigabitEthernet 0/0)#

	C(config-if-GigabitEthernet 0/0)# ipv6 address 2001:db8::3/32 C(config-if-GigabitEthernet 0/0)# ipv6 rip enable C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ipv6 address 2::1/64 C(config-if-GigabitEthernet 0/1)# ipv6 rip enable
Verification	Check the routing tables on Router A, Router B, and Router C. The routing tables should contain routes to a remote network that are learned through RIPng.
A	A# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::1/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:E7CE/128 via GigabitEthernet 0/0, local host
B	B# show ipv6 route IPv6 routing table name - Default - 6 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

	IA - Inter area R 2::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, GigabitEthernet 0/0 C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::2/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C9BA/128 via GigabitEthernet 0/0, local host
C	Ruijie# show ipv6 route IPv6 routing table name - Default - 9 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 2::/64 via GigabitEthernet 0/1, directly connected L 2::2/128 via GigabitEthernet 0/1, local host C 2001:DB8::/32 via GigabitEthernet 0/0, directly connected L 2001:DB8::3/128 via GigabitEthernet 0/0, local host C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:D521/128 via GigabitEthernet 0/1, local host

Common Errors

- The IPv6 address is not configured on an interface.
- The interface used for interconnection between devices is configured as a passive interface.

5.4.2 Advertising the Default Route or External Routes

Configuration Effect

- In the RIPng domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.
- In the RIPng domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIPng domain.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

↘ Configuring External Route Redistribution

- Optional.
- Perform this configuration if external routes of the RIPng domain should be introduced to the AS border router (ASBR).

↘ Generating a Default Route

- Optional.
- Perform this configuration if the default route should be introduced to an ASBR so that other routers in the RIPng domain access other AS domains through this ASBR by default.

Verification

- Run the **show ipv6 route rip** command on a non-ASBR to check whether the external routes of the domain and default route have been loaded.

Related Commands

↘ Advertising the Default Route to Neighbors on an Interface

Command	**ipv6 rip default-information** { **only**|**originate** } [**metric** *metric-value*]
Parameter Description	**only**: Advertises only IPv6 default route. **originate**: Advertises the IPv6 default route and other routes. **metric** *metric-value*: Indicates the metric of the default route. The value ranges from 1 to 15. The default value is 1.
Command Mode	Interface configuration mode
Usage Guide	After this command is configured on the interface, an IPv6 default route is advertised to the external devices through this interface, but the route itself is not added to the route forwarding table or the device and the RIPng route database. To prevent occurrence of a route loop, once this command is configured on an interface, RIPng refuses to receive the default route updates advertised by neighbors.

Redistributing Routes and Advertising External Routes to Neighbors

Command	**redistribute** { **connected | ospf** *process-id* **| static** } [**metric** *metric-value* | **route-map** *route-map-name*]
Parameter Description	**connected**: Indicates redistribution from direct routes. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value ranges from 1 to 65535. **static**: Indicates redistribution from static routes. **metric** *metric-value*: Sets the metric of the route redistributed to the RIPng domain. **route-map** *route-map-name*: Sets the redistribution filtering rules.
Command Mode	Routing process configuration mode
Usage Guide	During route redistribution, it is not necessary to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use completely different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other.

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router B, configure redistribution of static routes. ● On the GE0/1 interface of Router A, configure advertisement of the default route.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)# ipv6 rip default-information originate`
B	`B# configure terminal` `B(config)# ipv6 router rip` `B(config-router)# redistribute static`
Verification	● Check the routing tables on Router A and Router B, and confirm that Router A can learn the route 3001:10:10::/64, and Router B can learn the default route ::/0.

A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 3001:10:10::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1
B	B# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R ::/0 [120/2] via FE80::21A:A9FF:FE41:5B06, GigabitEthernet 0/1

5.4.3 Setting Route Filtering Rules

Configuration Effect

- Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

↘ Filtering the Received RIP Routing Information

- To refuse receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.

Filtering the Sent RIP Routing Information

- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.

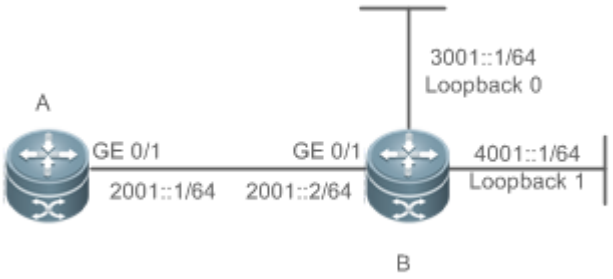
Verification

- Run the **show ipv6 route rip** command to check that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Command	**distribute-list prefix-list** *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]
Parameter Description	**prefix-list** *prefix-list-name:* Indicates the name of the prefix list, which is used to filter routes. **in** | **out:** Specifies update routes (received or sent routes) that are filtered. *interface-type interface-name:* Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Usage Guide	N/A

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On router A, configure route filtering.
A	`A# configure terminal` `A(config)# ipv6 prefix-list hello permit 4001::/64` `A(config)# ipv6 router rip` `A(config-router)# distribute-list prefix-list hello in`
Verification	● Check that Router A can learn only the route to 4001::/64.

A	A# show ipv6 route rip IPv6 routing table name - Default - 17 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area R 4001::/64 [120/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

5.4.4 Modifying Route Selection Parameters

Configuration Effect

- Change the RIPng routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects various types of routes so as to change the priorities of RIPng routes.

Notes

- The RIPng basic functions must be configured.

Configuration Steps

↘ Modifying the Administrative Distance of a RIPng Route

- Optional.
- Perform this configuration if you wish to change the priorities of RIPng routes on a router that runs multiple unicast routing protocols.

↘ Modifying the Metric Offset on an Interface

- Optional.
- Unless otherwise required, perform this configuration on a router where the metrics of routes need to be adjusted.

↘ Configuring the Default Metric of an External Route Redistributed to RIPng

- Optional.
- Unless otherwise required, perform this configuration on an ASBR to which external routes are introduced.

Verification

- Run the **show ipv6 rip** command to display the administrative distance of RIPng routes.
- Run the **show ipv6 rip data** command to display the metrics of external routes redistributed to RIPng.

Related Commands

Modifying the Administrative Distance of a RIPng Route

Command	**distance** *distance*
Parameter Description	*distance*: Sets the administrative distance of a RIPng route. The value is an integer ranging from 1 to 254.
Command Mode	Routing process configuration mode
Usage Guide	Run this command to set the administrative distance of a RIPng route.

Modifying the Metric Offset on an Interface

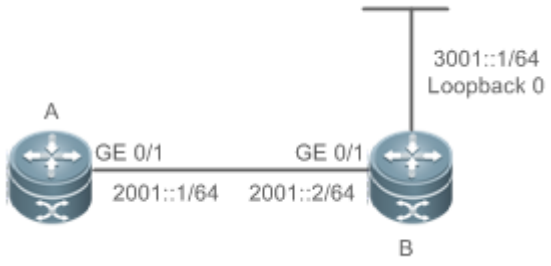
Command	**ipv6 rip metric-offset** *value*
Parameter Description	*value*: Indicates the interface metric offset. The value ranges from 1 to 16.
Command Mode	Routing process configuration mode
Usage Guide	Before a route is added to the routing table, the metric of the route must be added with the metric offset set on the interface. You can control the use of a route by setting the interface metric offset.

Configuring the Default Metric of an External Route Redistributed to RIPng

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric. The valid value ranges from 1 to 16. If the value is equal to or greater than 16, the RGOS determines that this route is unreachable.
Command Mode	Global configuration mode
Usage Guide	If the metric is not specified during redistribution of a routing protocol process, RIPng uses the metric defined by the **default-metric** command. If the metric is specified, the metric defined by the **default-metric** command is overwritten by the specified metric. If this command is not configured, the value of **default-metric** is 1.

Configuration Example

Modifying the Administrative Distance of a RIPng Route

Scenario	

Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, set the administrative distance of a RIPng route to 160.
	A# configure terminal A(config)# ipv6 router rip A(config-router)# distance 160
Verification	● On Router A, check whether the administrative distance of a RIPng route is 160.
	A# show ipv6 route rip | in 3001::/64 R 3001::/64 [160/2] via FE80::2D0:F8FF:FE22:334A, GigabitEthernet 0/1

5.4.5 Modifying Timers

Configuration Effect

- Change the duration of RIPng timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- The RIPng basic functions must be configured.
- Modifying the protocol control parameters may result in protocol running failures. Therefore, you are advised not to modify the timers.

Configuration Steps

↘ Modifying the Update Timer, Invalid Timer, and Flush Timer

- Mandatory.
- Unless otherwise required, perform this configuration on a router where RIPng timers need to be modified.

Verification

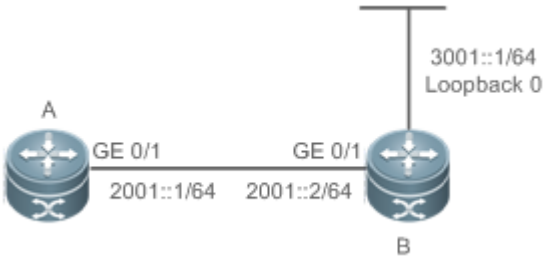
- Run the **show ipv6 rip** command to display settings of timers.

Related Commands

Command	**timers** *update invalid flush*
Parameter Description	*Update:* Indicates the route update time in second. It defines the interval at which the device sends the route update packet. Each time an update packet is received, the invalid timer and flush timer are reset. By default, a route update packet is sent every 30s. *Invalid:* Indicates the route invalid time in second, counted from the last time when a valid update packet is received. It defines the time after which the route in the routing list becomes invalid because the route is not

	updated. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the update packet is received before the invalid timer expires, the timer is reset. The default duration of the invalid timer is 180s. *Flush:* Indicates the route flushing time in second, counted from the time when the RIPng route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Usage Guide	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Configuration Example

Scenario	
Configuration Steps	● Configure the interface IPv6 addresses on all routers. (Omitted) ● Configure the RIPng basic functions on all routers. (Omitted) ● On Router A, configure the update timer, invalid timer, and flush timer.
B	`B# configure terminal` `B(config)# ipv6 router rip` `B(config-router)# timers 10 30 90`
Verification	● On Router B, check the settings of RIPng timers.

B	B# show ipv6 rip Routing Protocol is "RIPng" Sending updates every 10 seconds with +/-50%, next due in 12 seconds Timeout after 30 seconds, garbage collect after 90 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not set Default redistribution metric is 1 Default distance is 120 Redistribution: Redistributing protocol connected Default version control: send version 1, receive version 1 Interface Send Recv GigabitEthernet 0/1 1 1 Routing Information Sources: Gateway: fe80::2d0:f8ff:fe22:334a Distance: 120 Last Update: 00:00:02 Bad Packets: 0 Bad Routes: 0

Common Errors

- Settings of RIPng timers on devices connected to the same network are inconsistent. Consequently, routes cannot be learned properly.

5.4.6 Configuring Super VLAN to Enable RIPng

Configuration Effect

- Run the RIPng protocol on super VLANs.

Notes

- The RIPng basic functions must be configured.
- The designated sub VLAN is connected with neighbors.

Configuration Steps

↘ Running RIPng on Super VLAN

- Optional. Run this command to enable RIPng on a super VLAN if required.

Verification

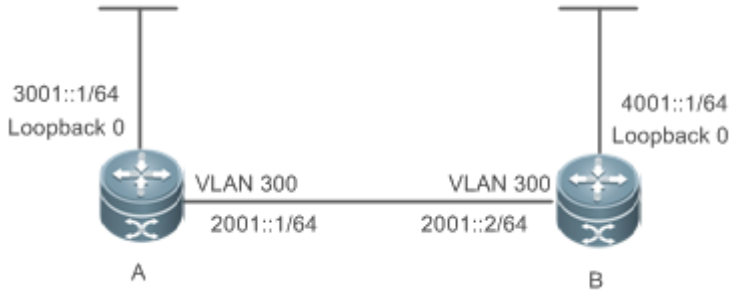
- Run the **show ipv6** route rip command to display the protocol status.

Related Commands

Running RIPng on Super VLAN

Command	**ipv6 rip subvlan [all |** *vid***]**
Parameter Description	**all:** Indicates that packets are allowed to be sent to all sub VLANs. *vid:* Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Command Mode	Interface configuration mode
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.

Configuration Example

Scenario **1-12**	
Configuration Steps	● Enable Ipv6 on interfaces of all devices. ● Configure the RIPng basic functions on all devices. ● Specify a particular sub VLAN on all devices.
A	`A# configure terminal` `A(config)# interface VLAN 300` `A(config-if-VLAN 300)# ipv6 rip subvlan 1024`

B	B# configure terminal B(config)# interface VLAN 300 B(config-if-VLAN 300)# ipv6 rip subvlan 1024
Verification	● Verify that the entry 4001::/64 has been loaded to the routing table on Device A. ● Verify that the entry 3001::/64 has been loaded to the routing table on Device B.
A	A# show ipv6 route rip R 4001::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, VLAN 300
B	A# show ipv6 route rip R 3001::/64 [120/2] via FE80::2D0:F8FF:FEFB:D521, VLAN 300

5.5 Monitoring

Displaying

Description	Command
Displays information about the RIPng process.	**show ipv6 rip**
Displays the RIPng routing table.	**show ipv6 rip database**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs RIPng.	**debug ipv6 rip** [interface *interface-type interface-num* | nsm | restart | event [ipsec]]

6 Configuring OSPFv2

6.1 Overview

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that is used within the Autonomous System (AS) to allow routers to obtain a route to a remote network.

OSPF Version 2 (OSPFv2) is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, notifications can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be L3 switches, routers, firewall, or wireless.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

Protocols and Standards

RFC2328	This memo documents version 2 of the OSPFprotocol. OSPF is a link-state routing protocol.
RFC 2370	This memo defines enhancements to the OSPFprotocol to support a new class of link-stateadvertisements (LSA) called Opaque LSAs.Opaque LSAs provide a generalized mechanismto allow for the future extensibility of OSPF.
RFC3137	This memo describes a backward-compatibletechnique that may be used by OSPF (OpenShortest Path First) implementations to advertiseunavailability to forward transit traffic or to lowerthe preference level for the paths through such arouter.
RFC3623	This memo documents an enhancement to theOSPF routing protocol, whereby an OSPF routercan stay on the

	forwarding path even as its OSPFsoftware is restarted.
RFC3630	This document describes extensions to the OSPFprotocol version 2 to support intra-area TrafficEngineering (TE), using Opaque Link StateAdvertisements.
RFC3682	The use of a packet's Time to Live (TTL) (IPv4)or Hop Limit (IPv6) to protect a protocol stackfrom CPU-utilization based attacks has beenproposed in many settings.
RFC3906	This document describes how conventional hop-by-hop link-state routing protocols interact withnew Traffic Engineering capabilities to createInterior Gateway Protocol (IGP) shortcuts.
RFC4576	This document specifies the necessary procedure,using one of the options bits in the LSA (Link StateAdvertisements) to indicate that an LSA hasalready been forwarded by a PE and should beignored by any other PEs that see it.
RFC4577	This document extends that specification byallowing the routing protocol on the PE/CEinterface to be the OSPF protocol.
RFC4750	This memo defines a portion of the ManagementInformation Base (MIB) for use with networkmanagement protocols in TCP/IP-based Internets.In particular, it defines objects for managingversion 2 of the Open Shortest Path First RoutingProtocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

6.2 Applications

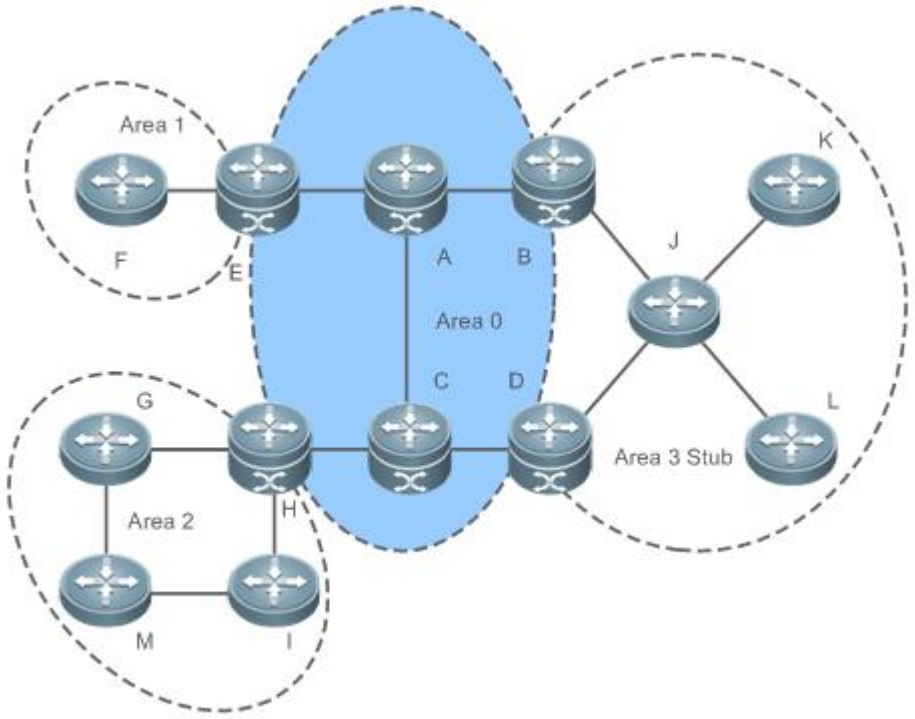
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.

6.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal arealocated on the stub be configured as a stub area. As shown in Figure 5-1, the network is divided into four areas. Communication between these areas must go through the backbone area, that is area 0.

Figure 5-1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

6.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, the AS is also called routing domain.

An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

OSPF supports multiple instances, and each instance corresponds to an OSPF process.

One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.

The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

RouterID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.

If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

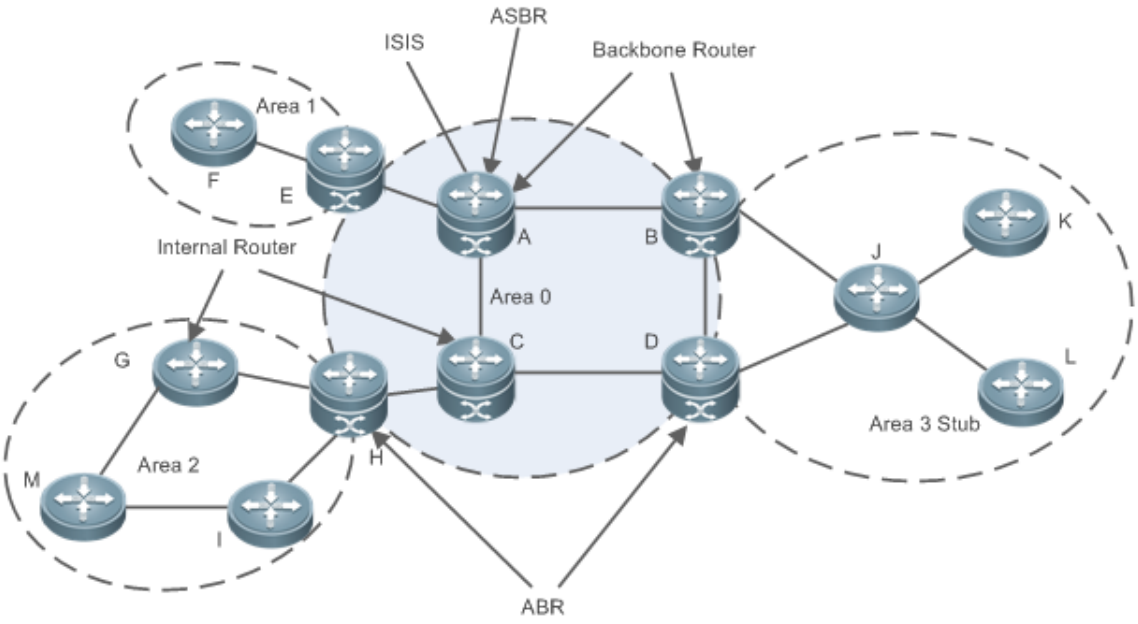
Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.

Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

Figure 5-2 Division of the OSPF Areas



OSPF Router

The following types of routers are defined in OSPF, and assigned with different responsibilities:

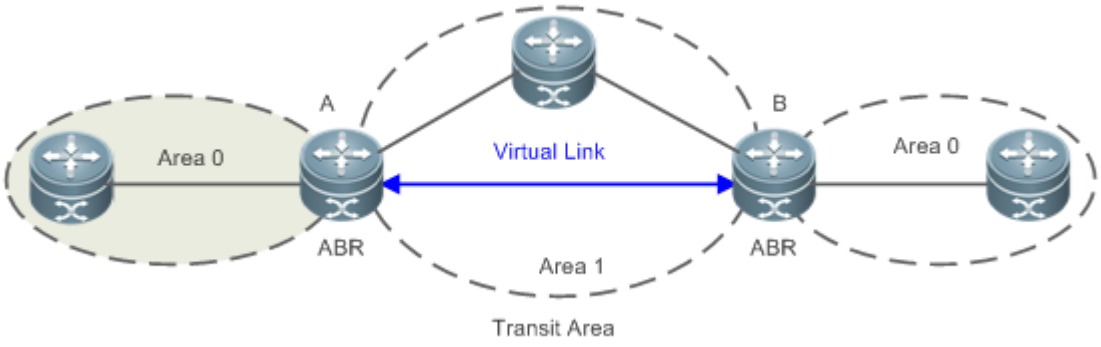
- Internal router
  All interface of an interval router belong to the same OSPF area. As shown in Figure 1-3, A, C, F, G, I, M, J, K, and L are internal routers.

- Area border router (ABR)
  An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. As shown in Figure 1-3, B, D, E, and H are ABRs.
- Backbone router
  A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers. As shown in Figure 5-, A, B, C, D, E, and H are backbone routers.
- AS boundary router (ASBR)
  An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. As shown in Figure 1-3, A is an ASBR.

Virtual Link

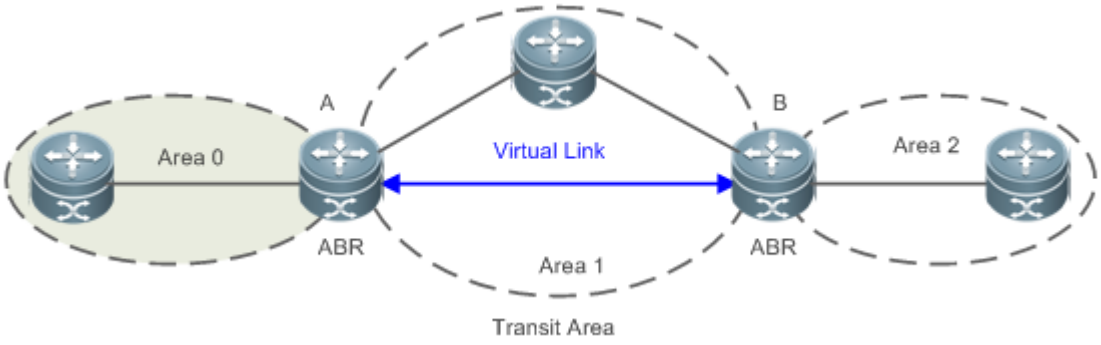
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 5-3 Discontinuous Backbone Area on the Physical Network



As shown in Figure 5-, a virtual link is set up between A and B to connect two separated area 0s. Area 1 is a transit area, and A and B are ABRs of area 1.

Figure 5-4 Failure to Directly Connect a Normal Area to the Backbone Areaon the Physical Network



As shown in Figure 5-, a virtual link is set up between A and B to extend area 0 to B so that area 0 can be directly connected to area 2 on B. Area 1 is a transit area, A is an ABR of area 1, and B is an ABR of area 0 and area 2.

LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type 1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA(Type 2)	This LSA is originated by a designated routers (DR) on the NBMA network. It describes the link state in the current network segment, and is advertised only within the area where the DR is located.
Network-summary-LSA(Type 3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas or Not-So-Stubby Area (NSSA) areas.
ASBR-summary-LSA(Type 4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except areas where the ASBR is located.
AS-external-LSA(Type 5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type 7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
Opaque LSA(Type 9/Type 10/Type 11)	Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF, wherein, ● Type 9 LSAs are only advertised within the network segment where interfaces resides. The Grace LSA used to support graceful restart (GR) is one of Type 9 LSAs. ● Type 10 LSAs are advertised within an area. The LSA used to support Traffic Engineering (TE) is one of Type 10 LSAs. ● Type 11 LSAs are advertised within an AS. At present, there are no application examples of Type 11 LSAs.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets

	are sent only after DD packets are exchanged successfully between OSPF neighbors.
Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.
Enhanced Security and Reliability	Use authentication to enhance security, stability, and reliability of OSPF.
Network Management	Use functions such as the management information base (MIB) and Syslog to facilitate OSPF management.

6.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
  An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
  A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- Shortest Path Tree (SPT) computation → Formation of a routing table
  The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

Working Principle

↘ Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Subnet mask of the originating router interface (or virtual link)
- Authentication information of the originating router interface (or virtual link)

- Hello interval of the originating router interface (or virtual link)
- Neighbor dead interval of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- IP addresses of the DR and Backup Designated Router (BDR)
- Router ID of the neighbor of the originating router

Database Synchronization → Full Adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

OSPF will be very quiet without changes in link costs or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

SPT Computation → Formation of a Routing Table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

OSPF Network Types

A router does not necessarily need to exchange LSAs with every neighbor and set upan adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set upan adjacency:

- Broadcast
  Neighbors are discovered, and the DR and BDR are elected.
  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
  Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.
- Non-broadcast multiple access (NBMA)
  Neighbors are manually configured, and the DR and BDR are elected.
  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other

routers do not exchange LSAs with each other, and the adjacency is not set up.

X.25, frame relay, and ATM belong to NBMA networks by default.

- Point-to-point (P2P)

  Neighbors are automatically discovered, and the DR or BDR is not elected.

  LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.

  PPP,HDLC, and LAPB belongs to the P2P network type by default.

- Point-to-multipoint (P2MP)

  Neighbors are automatically discovered, and the DR or BDR is not elected.

  LSAs are exchanged between any two routers, and the adjacency is set up.

  Networks without any link layer protocol belong to the P2MP network type by default. P2MP broadcast

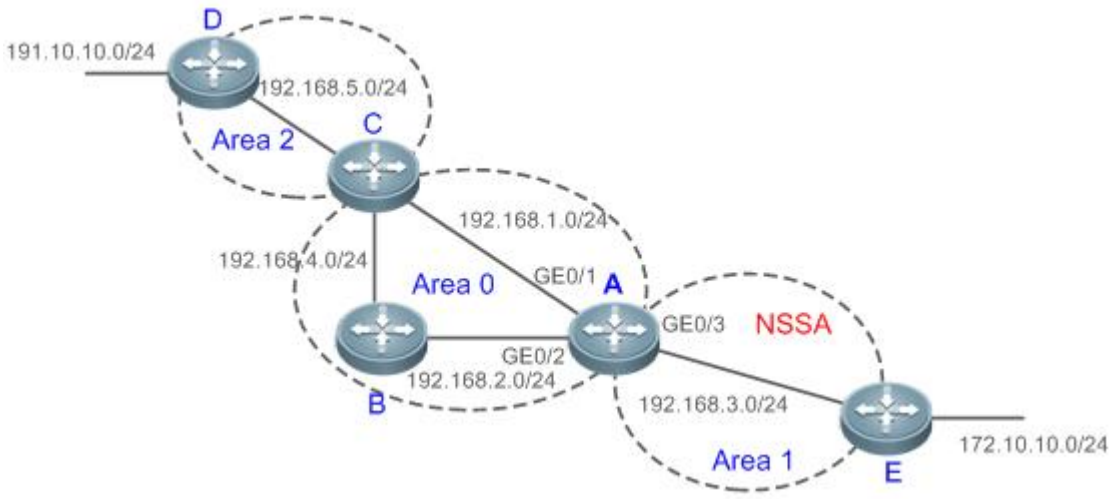
  Neighbors are manually configured, and the DR or BDR is not elected.

  LSAs are exchanged between any two routers, and the adjacency is set up.

  Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 5-5



Display the OSPF routes (marked in red) in the routing table of Router A.

```
A#show ip route


Codes:  C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00,GigabitEthernet 0/3
O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26,GigabitEthernet 0/1
C    192.168.1.0/24 is directly connected,GigabitEthernet 0/1
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected,GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
C    192.168.3.0/24 is directly connected,GigabitEthernet 0/3
C    192.168.3.1/32 is local host.
O    192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02,GigabitEthernet 0/2
O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02,GigabitEthernet 0/1
```

A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Intra-area route
  This type of route describes how to arrive ata destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- IA: Inter-area route
  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- E1: Type 1 external route
  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- E2: Type 2 external route
  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- N1: Type 1 external route of the NSSA area
  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.
- N2: Type 2 external route of the NSSA area
  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

Reliability of E2 and N2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **router ospf** 1 command to create an OSPF process on the router.

Run the **network area** command to enable OSPF on the interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ip ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).

Run the **ip ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.

Use the **poll-interval** parameter in the **neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.

Run the **ip ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.

Run the **ip ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.

Use the **hello-interval** parameter in the **area virtual-link**command to modify the Hello interval on the virtual link. The default value is 10s.

Use the **dead-interval** parameter in the **area virtual-link**command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.

Use the **transmit-delay** parameter in the **area virtual-link**command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.

Use the **retransmit-interval** parameter in the **area virtual-link**command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.

Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.

Run the **timerspacinglsa-group** command to modify the LSA group update interval. The default value is 30s.

Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.

Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.

Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

↘ OSPF Network Types

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Run the **ip ospf network** command to manually specify the network type of an interface.

Run the **neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.

Run the **ip ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

6.3.2 OSPF Route Management

Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

↘ (Totally) Stub Area and (Totally)NSSA Area

The (totally) stub and (totally)NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type1 and Type2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one	Allowed	Not allowed	Allowed

		default route)			
Totally NSSA area	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

- The ABR uses Type 3LSAs to advertise a default route to the (totally) stub or NSSA area.
- The ABR converts Type 7 LSAs in the totally NSSA area to Type 5LSAs, and advertise Type5LSAs to the backbone area.

- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of E1, E2, and IA routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area IA: a route to a destination network in another area E1 or E2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)

Route Redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

Default Route Introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs. If continuous network segments exist, it is recommended that you configure route summarization.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase.To prevent these problems, the ABR or ASBR automatically adds a discard route to the routing table. This route will not be advertised.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.

Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information advertised between areas: Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process(Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path. The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

Using configuration commands, you can modify the link costs:

- Cost from an interface to a directly connected network segment and cost from the interface to a neighbor
- Costfrom an ABR to the inter-area summarization network segment and cost from the ABR to the default network segment
- Costfrom an ASBR to an external network segment and cost from the ASBR to the default network segment

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Route Source	Directly-Connected Network	Static Route	OSPF Route	RIP Route	Unreachable Route
Default AD	0	1	110	120	255

Related Configuration

Stub Area and NSSA Area

No stub or NSSA area is configured by default.

Run the **area stub** command to configure a specified area as a stub area.

Run the **area nssa** command to configure a specified area as an NSSA area.

- The backbone area cannot be configured as a stub or an NSSA area.
- A transit area (with virtual links going through) cannot be configured as a stub or an NSSA area.
- An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce the default route.

After configuring route redistribution and default route introduction, the route automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **arearange** command to summarize routes distributed between areas (Type 3 LSA) on the ABR.

Run the **summary-address** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Run the **discard-route** command to add a discard route to the routing table.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Run the **ip ospfdatabase-filter all out** command to prohibit an interface from sending routing information (any LSAs).

Run the **area filter-list** command to filter routing information advertised between areas on the ABR. Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
  The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
  Run the **auto-costreference-bandwidth** command to set the reference bandwidth of auto cost. The default value is 100 Mbps.
  Run the **ip ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
  The default value is the auto cost.
  Use the **cost** parameter in the **neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
  This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the inter-area summarization network segment (that is, the cost of the summarized inter-area route)
  If OSPF routing is compatible with RFC1583, the default value is the minimum cost among all costs of the summarized links; otherwise, the default value is the maximum cost among all costs of the summarized links.
  Run the **compatible rfc1583** command to make OSPF routing compatible with RFC1583. By default, OSPF routing is compatible with RFC1583.
  Use the **cost** parameter in the **area range** command to modify the cost of inter-area route summarization.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)
  The default value is 1.
  Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub or NSSA areas.
- Cost from the ASBR to an external network segment (that is, the metric of an external route)
  By default, the metric of other types of redistributed routes is 20, and the route type is Type 2 External.
  Run the **default-metric** command to modify the default metric of the external route.
  Use the **metric**, **metric-type** and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.

- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
  By default, the metric is 1, and the route type is Type 2 External.
  Use the **metric**, **metric-type** and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.
  Use the **metric** and **metric-type** parametersof**default-information originate**in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.
- Run the **max-metric router-lsa** command to set metrics of all routes advertised on the router to the maximum value. In this way, the total cost of any path that passes through this router will become very large, and the path can hardly become the shortest path.

OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

6.3.3 Enhanced Security and Reliability

Use authentication to enhance security, stability, and reliability of OSPF.

Working Principle

Authentication

Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. OSPF packets received on the OSPF interface (or at both ends of the virtual link) are authenticated. If authentication fails, the packets are discarded and the adjacency cannot be set up.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

MTU Verification

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

Source Address Verification

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet.

In some scenarios, the source address of a packet received by OSPF maynot be in the same network segment as the receiving interface, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be

obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Two-Way Maintenance

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

Concurrent Neighbor Interaction Restriction

When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

Overflow

OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

The overflow function limit the number of external routes in the LSDB to control the size of the LSDB.

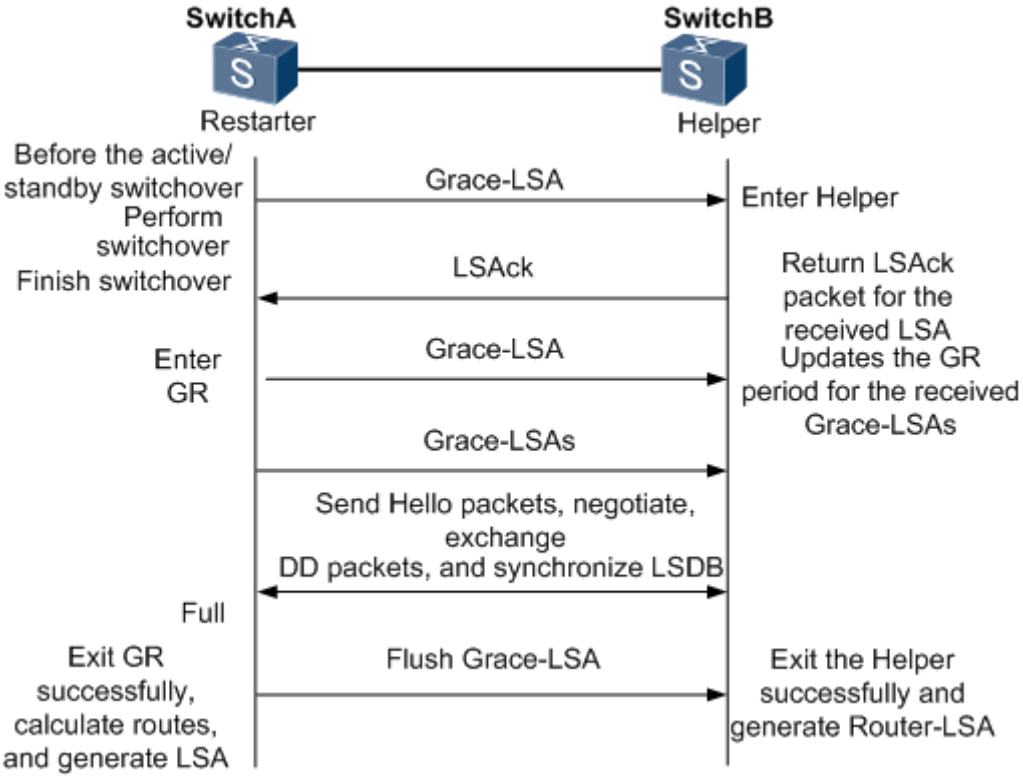
When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 5-6 Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a Grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the Full state, the router can exit the GR process successfully.

Related Configuration

↘ OSPF Packet Authentication

By default, authentication is disabled.

- Run the **areaauthentication** command to enable the authentication function in the entire area so that the function takes effect on all interfaces in this area. If authentication is enabled in area 0, the function takes effect on the virtual link.
- Run the **ip ospf authentication** command to enable authentication on an interface. This configuration takes precedence over the area-based configuration.
- Run the **ip ospf authentication-key** command to set the text authentication key on an interface.
- Run the **ip ospfmessage-digest-key** command to set the message digest 5 (MD5) authentication key on an interface.

- Use the **authentication** parameter in the **area virtual-link** command to enable authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.
- Use the **authentication-key** parameter in the **area virtual-link** command to set the text authentication key at both ends of a virtual link.
- Use the **message-digest-key** parameter in the **area virtual-link** command to set the MD5 authentication key at both ends of a virtual link.

MTU Verification

By default, MTU verification is disabled.

Run the **ip ospf mtu-ignore** command to disable MTU verification on an interface.

Source address verification

By default, source address verification is enabled on a P2P interface.

Run the **ip ospf source-check-ignore** command to disable source address verification on an interface.

Two-Way Maintenance

By default, bidirectional maintenance is enabled.

Run the **two-way-maintain** command to enable two-way maintenance.

Concurrent neighbor Interaction Restriction

Run the **max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with the current OSPF process. The default value is 5.

Run the **ipv6 router ospf max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with all OSPF processes on the router. The default value is 10.

Overflow

Run the **overflow memory-lack** command to allow the router to enter the overflow state when the memory is insufficient. By default, the router is allowed to enter the overflow state when the memory is insufficient.

Run the **overflow database** command to allow the router to enter the overflow state when the number of LSAs is too large. By default, the router is not allowed to enter the overflow state when the number of LSAs is too large.

Run the **overflow database external** command to allow the router to enter the overflow state when the number of externalLSAs is too large. By default, the router is not allowed to enter the overflow state when the number of external-LSAs is too large.

GR

By default, the restarter function is disable, and the helper function is enabled.

Run the **graceful-restart** command to configure the restarter function.

Run the **graceful-restart helper** command to configure the helper function.

6.3.4 Network Management

Use functions such as the MIB and Syslog to facilitate OSPF management.

Working Principle

MIB

MIB is the device status information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound with only one OSPF process.

Trap

A Trap message is a notification generated when the system detects a fault. This message contains the related fault information.

If the Trap function is enabled, the router can proactively send the Trap messages to the network management device.

Syslog

The Syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the Syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process that the OSPF adjacency is set up and maintained.

Related Configuration

MIB

By default, the MIB is bound with the OSPF process with the smallest process ID.

Run the **enable mib-binding** command to bind the MIB with the current OSPF process.

Trap

By default, all traps are disabled, and the device is not allowed to send OSPF traps.

Run the **enable traps** command to enable a specified trap for an OSPF process.

Run the **snmp-server enable traps ospf** command to allow the device to send OSPF traps.

SYSLOG

By default, the Syslog is allowed to record the adjacency changes.

Run the **log-adj-changes** command to allow the Syslog to record the adjacency changes.

6.4 Configuration

Configuration	Description and Command	
Configuring OSPF Basic Functions	⚠ (Mandatory) It is used to build an OSPF routing domain.	
	routerospf	Creates an OSPF process.
	router-id	Configures a router ID.
	network area	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	⚠ (Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ip ospf network	Defines the network type.
	neighbor	Specifies a neighbor.
	ip ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	⚠ (Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring Stub Area and NSSA Area	⚠ (Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	areastub	Configures a stub area.
	areanssa	Configures an NSSA area.
Configuring Route Summarization	⚠ (Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	arearange	Summarizes routes that are advertised between areas.
	summary-address	Summarizes routes that are introduced through redistribution.
	discard-route	Adds a discard route to the routing table.
Configuring Route Summarization	⚠ (Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	ip ospfdatabase-filter all out	Prohibits an interface from sending LSAs.
	area filter-list	Filters routes that are advertised between areas..

Configuration	Description and Command	
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-listin	Filters routes that are calculated based on the received LSAs.
Configuring Route Filtering	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-costreference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ip ospf cost	Modifies the cost in the outbound direction of an interface.
	areadefault-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	max-metric router-lsa	Configures the maximum metric.
	compatible rfc1583	Enables the routing rules to be compatible with RFC1583.
	distance	Modifies the OSPF AD.
Modifying Route Cost and AD	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	areaauthentication	Enables authentication and sets the authentication mode in an area.
	ip ospf authentication	Enables authentication and sets the authentication mode on an interface.
	ip ospf authentication-key	Sets the text authentication key on an interface.
	ip ospfmessage-digest-keymd5	Sets the MD5 authentication key on an interface.
Enabling Authentication	(Optional) It is used to prevent the problem that OSPF processes stop running due to over-consumption of the memory.	
	overflow memory-lack	Allows the router to enter the overflow state when the memory is insufficient.
	overflow database	Allows the router to enter the overflow state when the number of LSAs exceeds the preset limit.

Configuration	Description and Command	
	overflow database external	Allows the router to enter the overflow state when the number of external LSAs exceeds the preset limit.
Enabling Overflow	(Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	
	max-concurrent-dd	Modifies the maximum number of con current neighbors on the current OSPF process.
	router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.
Modifying the Maximum Number of Concurrent Neighbors	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to the failure to obtain the peer address.	
	ip ospf source-check-ignore	Disables source address verification on an interface.
Disabling Source Address Verification	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ip ospf mtu-ignore	Disables MTU verification on an interface.
Disabling MTU Verification	(Optional) It is used to prevent termination of the adjacencydue to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling Two-Way Maintenance	(Optional) It is used to retain OSPF routing forwarding during restart or active/standby switchover of the OSPF processes to prevent traffic interruption.	
	graceful-restart	Configures the restarter function.
	graceful-restart helper	Configures the helper function.
Configuring the Network Management Function	(Optional) The configurations enable users to use the SNMP network management software to manage OSPF.	
	enable mib-binding	Binds the MIB with the current OSPF process.
	enable traps	Enables a specified trap for an OSPF process.
	snmp-server enable traps ospf	Allows the device to send OSPF traps.
	log-adj-changes	Allows the Syslog to record the adjacency changes.
Modifying Protocol	(Optional) You are advised not to modify protocol control parameters unless necessary.	

Configuration	Description and Command	
Control Parameters	**ip ospf hello-interval**	Modifies the Hello interval.
	ip ospf dead-interval	Modifies the neighbor death interval.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the external route computation delay.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	ip ospf transmit-delay	Modifies the LSU packet transmission delay.
	ip ospf retransmit-interval	Modifies the LSU packet retransmission interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.

6.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

Notes

- Ensure that the IP unitcast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- It is strongly recommended that you manually configure the router ID.
- After **ip ospf disable all** is configured, the interface neither sends or receives any OSPF packet, nor participates in OSPF computation even if the interface belongs to the network.

Configuration Steps

↘ Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

↘ Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.

- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Enabling OSPF on an Interface and Specifying an Area ID

- Mandatory.
- The configuration is mandatory for every router.

Verification

- Run the **show ip route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv4 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**router ospf** *process-id*
Parameter Description	*process-id:* Indicates the OSPF process ID. If the process ID is not specified, the process ID is 1.
Command Mode	Global configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently.

Configuring a Router ID

Command	**router-id***router-id*
Parameter Description	*router-id:* Indicates the router ID to be configured. It is expressed in the IP address.
Command Mode	OSPF routing process configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently. Each OSPF process uses a unique router ID.

Enabling OSPF on an Interface and Specifying an Area ID

Command	**network***ip-addresswildcard***area***area-id*
Parameter Description	*ip-address*: Indicates the IP address of the interface. *wildcard:* Indicates the IP address comparison mode. **0** indicates accurate matching, and **1** indicates that no comparison is performed. *area-id:* Indicates the ID of an OSPF area. An OSPF area is always associated with an address range. To facilitate management, you can use a subnet as the ID of an OSPF area.

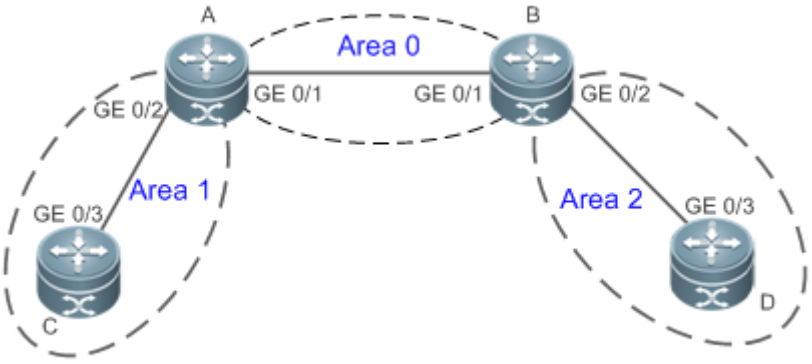
Command Mode	OSPF routing process configuration mode
Usage Guide	By defining *ip-address* and *wildcard*, you can use one command to associate multiple interfaces with one OSPF area. To run OSPF on one interface, you must include the primary IP address of the interface in the IP address range defined by **network area**. If the IP address range defined by **network area** contains only the secondary IP address of the interface, OSPF does not run on this interface. If the interface address matches the IP address ranges defined in the **network** commands of multiple OSPF processes, the OSPF process that the interface is associated with is determined based on the best match method.

Creating a Virtual Link

Command	**area** *area-id***virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**dead-interval** *seconds*] [**hello-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [[**authentication-key**[**0** |**7**]*key*] | [**message-digest-key***key-id* **md5**[**0** |**7**]*key*]]
Parameter Description	*area-id:* Indicates the ID of the OSPF transit area. The area ID can be a decimal integer or an IP address. *router-id:* Indicates the ID of a neighborrouter on the virtual link. **dead-interval***seconds:* Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647. The setting of this parameter must be consistent with that on a neighbor. **hello-interval** *seconds:* Indicates the interval at which OSPF sends the Hello packet to the virtual link. The unit is second. The value ranges from 1 to 65,535. The setting of this parameter must be consistent with that on a neighbor. **retransmit-interval** *seconds:* Indicates the OSPF LSA retransmission time. The unit is second. The value ranges from 1 to 65,535. **transmit-delay** *seconds:* Indicates the delay after which OSPF sends the LSA. The unit is second. The value ranges from 1 to 65,535. **authentication-key** [**0** | **7**]*key:* Defines the key for OSPF plain text authentication. **message-digest-key** *key-id***md5** [**0** | **7**]key: Defines the key ID and key for OSPF MD5 authentication. **authentication:** Sets the authentication type to plain text authentication. **message-digest:** Sets the authentication type to MD5 authentication. **null:** Indicates that authentication is disabled.
Command Mode	OSPF routing process configuration mode
Usage Guide	In the OSPF routing domain, all areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA area cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas. **router-id** is the ID of an OSPF neighbor router. If you are sure about the value of **router-id**, run the **show ip ospf neighbor** command to confirm the value. You can configure the loopback address as the router ID. The **area virtual-link** command defines only the authentication key of the virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, you must run the **area authentication**

	command.

Configuration Example

Scenario	 **Remarks** The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/3 192.168.2.2 D: GE 0/3 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. ● Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.) ● Configure the OSPF instances and router IDs on all routers. ● Enable OSPF on the interfaces configured on all routers.
A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)#exit A(config)#router ospf 1 A(config-router)#router-id192.168.1.1 A(config-router)#network 192.168.1.0 0.0.0.255 area 0

	A(config-router)#network 192.168.2.0 0.0.0.255 area 1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)#exit B(config)#router ospf 1 B(config-router)#router-id192.168.1.2 B(config-router)#network 192.168.1.0 0.0.0.255 area 0 B(config-router)#network 192.168.3.0 0.0.0.255 area 2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0 C(config-if-GigabitEthernet 0/3)#exit C(config)#router ospf 1 C(config-router)#router-id192.168.2.2 C(config-router)#network 192.168.2.0 0.0.0.255 area 1
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0 D(config-if-GigabitEthernet 0/3)#exit D(config)#router ospf 1 D(config-router)#router-id192.168.3.2 D(config-router)#network 192.168.3.0 0.0.0.255 area 2
Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● On Router D, verify that the IP address 192.168.2.2 can be pinged successfully.

A	A# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:40192.168.1.2 GigabitEthernet 0/1 192.168.2.2 1 Full/BDR00:00:34 192.168.2.2 GigabitEthernet 0/2 A# show ip route ospf O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
B	B# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.1.1 GigabitEthernet 0/1 192.168.3.2 1 Full/BDR00:00:30 192.168.3.2 GigabitEthernet 0/2 B# show ip route ospf O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
C	C# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.2.1 GigabitEthernet 0/3 C# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
D	D# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.21 Full/BDR00:00:30 192.168.3.1 GigabitEthernet 0/3 D# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3

```
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3


D# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Common Errors

- OSPF cannot be enabled because the IP unicast routing function is disabled.
- The network segment configured by the **network** command does not include the interface IP addresses.
- The area IDs enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.
- The same interface IP address is configured on multiple routers, resulting in a running error of the OSPF network.

6.4.2 Setting the Network Type

Configuration Effect

- Run OSPF to provide the IPv4 unicast routing serviceif the physical network is X.25, frame relay, or ATM.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends OSPF packets in multicast mode. Neighbors are automatically discovered, and the DR/BDR election is required.
- The P2P network sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The NBMA network sends OSPF packets in unicast mode. Neighbors must be manually specified, and the DR/BDR election is required.
- The P2MP network (without the **non-broadcast** parameter) sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The P2MP network (with the **non-broadcast** parameter) sends OSPF packets in unicast mode. Neighbors must be manually specified.

Configuration Steps

↘ Configuring the Interface Network Type

- Optional.

- The configuration is required on routers at both ends of the link.

Configuring Neighbors

- (Optional) If the interface network type is set to NBMA or P2MP (with the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (with the **non-broadcast** parameter) network.

Configuring the Interface Priority

- (Optional) You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

Verification

- Run the **show ip ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ip ospf network** { **broadcast**| **non-broadcast**| **point-to-multipoint**[**non-broadcast**] | **point-to-point**}
Parameter Description	**broadcast**: Sets the interface network type to broadcast. **non-broadcast:** Sets the interface network type to non-broadcast. **point-to-multipoint** [**non-broadcast**]: Sets the interface network type to P2MP. If the interface does not have the broadcast capability, the **non-broadcast** parameter must be available. **point-to-point:** Sets the interface network type to P2P.
Command Mode	Interface configuration mode
Usage Guide	The broadcast type requires that the interface must have the broadcast capability. The P2P type requires that the interfaces are interconnected in one-to-one manner. The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other. The P2MP type does not raise any requirement.

Configuring Neighbors

Command	**neighbor** *ip-address* [**poll-interval***seconds*] [**priority***priority*] [**cost** *cost*]
Parameter Description	*ip-address*: Indicates the IP address of the neighbor interface. **poll-interval***seconds***:** Indicates the neighbor polling interval. The unit is second. The value ranges from 0 to 2,147,483,647. This parameter is applicable only to the NBMA interface. **priority***priority*: Indicates the neighbor priority. The value ranges from 0 to 255. This parameter is applicable only to the NBMA interface. **cost***cost***:** Indicates the cost required to reach each neighbor. There is no default value. The value ranges from 0 to 65,535. This parameter is applicable only to the P2MP interface.

Command Mode	OSPF routing process configuration mode
Usage Guide	Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. If a neighbor router becomes inactive on the NBMA network, OSPF still sends Hello packets to this neighbor even if no Hello packet is received within the router death time. The interval at which the Hello packet is sent is called polling interval. When running for the first time, OSPF sends Hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the Hello packets to all neighbors to set up the adjacency. The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must use this command to manually configure neighbors for the P2MP (non-broadcast) network. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

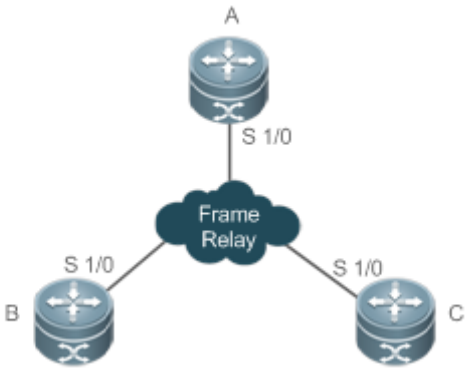
Configuring the Interface Priority

Command	**ip ospf priority** *priority*
Parameter Description	*priority*: Indicates the OSPF priority of an interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	The OSPF interface priority is contained in the Hello packet. When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does not participate in the DR/BDR election. This command is applicable only to the OSPF broadcast and NBMA interfaces.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Setting the Interface Network Type to P2MP

Scenario	 **Remarks** The interface IP addresses are as follows: A: S1/0 192.168.1.2 B: S1/0 192.168.1.3 C: S1/0 192.168.1.4
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the interface network type to P2MP on all routers.
A	`A#configure terminal` `A(config)# interface Serial1/0` `A(config-Serial1/0)# encapsulation frame-relay` `A(config-Serial1/0)# ip ospf network point-to-multipoint`
B	`B#configure terminal` `B(config)# interface Serial1/0` `B(config-Serial1/0)# encapsulation frame-relay` `B(config-Serial1/0)# ip ospf network point-to-multipoint`
C	`C#configure terminal` `C(config)# interface Serial1/0` `C(config-Serial1/0)# encapsulation frame-relay` `C(config-Serial1/0)# ip ospf network point-to-multipoint`

Verification	Verify that the interface network type is P2MP. A# show ip ospf interface Serial1/0 Serial1/0 is up, line protocol is up Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (with the **non-broadcast** parameter), but neighbors are not specified.

6.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- In the OSPF domain, introduce a unicast route to other AS domains so that the unicast routing service to other AS domainscan be provided for users in the OSPF domain.
- In the OSPF domain, inject a default route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ **Configuring External Route Redistribution**

- (Optional) This configuration is required if external routes of the OSPF domain should be introduced to an ASBR.
- This configuration is performed on an ASBR.

↘ **Generating a Default Route**

- (Optional) This configuration is required if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.
- This configuration is performed on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ip route** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ip route** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv4 unicast service to other AS domains is correct.

Related Commands

Configuring External Route Redistribution

Command	**redistribute** { **connected** |**ospf***process-id* | **rip** | **static**} [**match** {**internal** | **external** [**1**|**2**]| **nssa-external** [**1**|**2**]}] [**metric** *metric-value*] [**metric-type** {**1**|**2**}] [**route-map** *route-map-name*] [**subnets**] [**tag***tag-value*]
Parameter Description	**connected:** Indicates redistribution from direct routes. **ospf** *process-id:* Indicates redistribution from OSPF. *process-id* specifies an OSPF process. The value ranges from 1 to 65,535. **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes. **match:** Used only when OSPF routes are redistributed. Only the routes meeting the filtering conditions are redistributed. By default, all OSPF routes can be redistributed. **metric** *metric-value:* Specifies the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type { 1 | 2 }**: Setsthe external route type, which can be E-1 or E-2. **route-map** *route-map-name:* Setsthe redistribution filtering rules. **subnets:** Specifiesthe non-standard networks for redistribution. **tag** *tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type 5 LSAs to other OSPF routers in the domain. If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. For details, see the configuration example. If **route-map** is specified, the filtering rules specified in **route-map** are applicable to original parameters of redistribution. For redistribution of OSPF, the routemap is used for filtering only when the redistributed

	routes meet criteria specified by **match**. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Introducing a Default Route

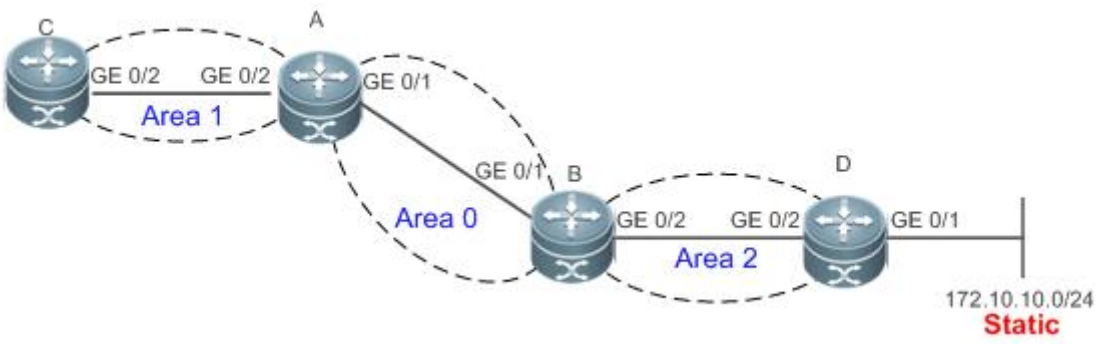
Command	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map-name*]
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. **metric-type***type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To have the ASBR generates a default route, configure the **default-information originate** command. If **always** is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ip ospf database** command to display the OSPF link status database. The external link with the ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command. OSPF has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ip route** command displays only the Type 1 route. A router in the stub area cannot generate an external default route. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring Static Route Redistribution

Scenario



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers. (Omitted)
- Configure the OSPF basic functions on all routers. (Omitted)
- Introduce an external static route to Router D.

D

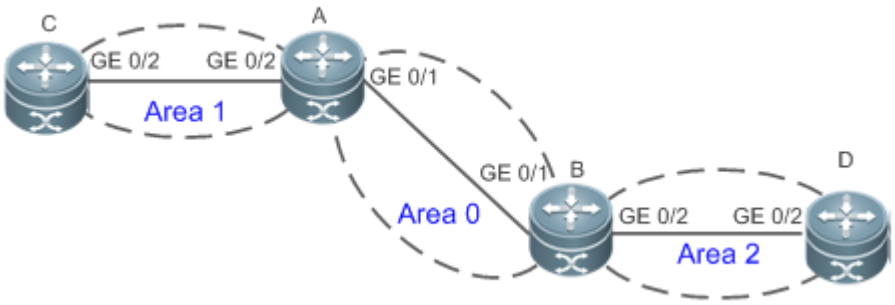
```
D# configure terminal
D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.3
D(config)#router ospf 1
D(config-router)# redistribute staticsubnets
```

Verification

- On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to an external route is generated.
- On Router C, run the **show ip route ospf** command to verify that the external static route has been introduced.

D	D# show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1) AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 172.10.10.0 192.168.22.30 11 0x80000001 0xa4bb E2 172.10.10.0/24 0
C	C# show ip route ospf O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

Configuring the Default Route

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the default route on Router D.
D	D# configure terminal D(config)#router ospf 1 D(config-router)#default-information originate always

Verification	• On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to the default route is generated. • On Router C, run the **show ip route ospf** command to verify that the OSPF default route exists.
D	D#show ip ospf database external brief OSPF Router with ID (192.168.22.30) (Process ID 1) AS External Link States Link ID ADV Router Age Seq# CkSum Route Tag 0.0.0.0 192.168.22.30 565 0x80000002 0xa190 E2 0.0.0.0/0 1
C	C# show ip route ospf O E20.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2

Common Errors

- The subnet route is not introduced because the **subnets** parameter in the **redistribute** command is not configured.
- A routing loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

6.4.4 Configuring Stub Area and NSSA Area

Configuration Effect

- Configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

Configuration Steps

↘ Configuring a Stub Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

↘ Configuring an NSSA Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area and introduce OSPF external routes to the area.
- The area must be configured as an NSSA area on all routers in this area.

Verification

Verifying the Stub Area

- On a router in the stub area, run the **show ip route** command to verify that the router is not loaded with any external routes.

Verifying the NSSA Area

- On a router in the NSSA area, run the **show ip ospf database** command to verify that the introduced external route generates Type 7 LSAs.
- On a router in the backbone area, run the **show ip route** command to verify that the router is loaded with external routes introduced from the NSSA area.

Related Commands

Configuring a Stub Area

Command	**area** *area-id* **stub** [**no-summary**]
Parameter Description	*area-id:* Indicates the ID of the stub area. **no-summary:** Prohibits the ABR from sending network summary LSAs. At this time, the stub can be called totally stub area. This parameter is configured only when the router is an ABR.
Command Mode	OSPF routing process configuration mode
Usage Guide	You must run the **area stub** command on all routers in the OSPF stub area. The ABR sends only three types of LSAs to the stub area: (1) Type 1: Router LSA; (2) Type 2: Network LSA; (3) Type 3: Network Summary LSA. From the routing table point of view, a router in the stub area can learn only the internal routes of the OSPF routing domain, including the internal default route generated by an ABR. A router in the stub area cannot learn external routes of the OSPF routing domain. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR. You can run either the **area stub** or **area default-cost** command to configure an OSPF area as a stub area. If **area stub** is used, you must configure this command on all routers connected to the stub area. If **area default-cost** is used, run this command only on the ABR in the stub area. The **area default-cost** command defines the initial cost (metric) of the internal default route.

Configuring an NSSA Area

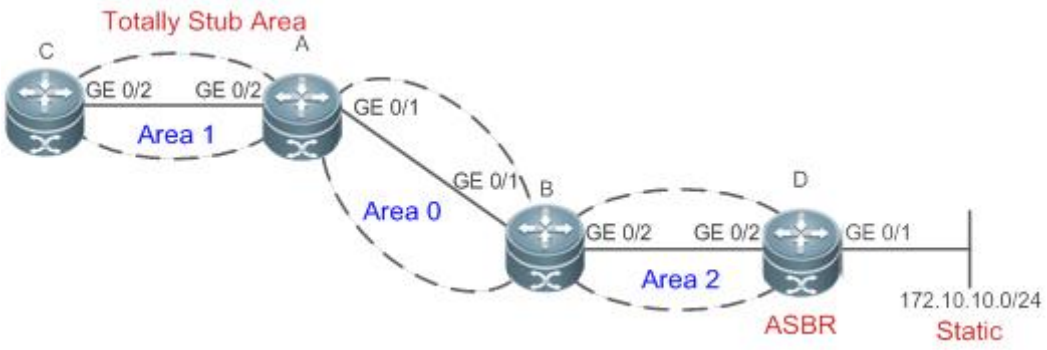
Command	**area***area-id* **nssa** [**no-redistribution**] [**default-information-originate**[**metric***value*] [**metric-type***type*]] [**no-summary**] [**translator** [**stability-interval***seconds* | **always**] **]**

Parameter Description	*area-id:* Indicates the ID of the NSSA area. **no-redistribution:** Select this option if the router is an NSSA ABR and you want to use only the **redistribute** command to introduce the routing information into a common area instead of an NSSA area. **default-information-originate:** Indicates that a default Type 7 LSA is generated and introduced to the NSSA area. This option takes effect only on an NSSA ABR or ASBR. **metric***value:* Specifies the metric of the generated default LSA. The value ranges from 0 to 16,777,214. The default value is 1. **metric-type***type:* Specifies the route type of the generated default LSA. The values include 1 and 2. **1** represents N-1, and **2** represents N-2. The default value is 2. **no-summary:** Prohibits the ABR in the NSSA area from sending summary LSAs (Type-3 LSA). **translator:** Indicatesthat the NSSA ABR is a translator. **stability-interval***seconds:* Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator. The unit is second. The default value is 40. The value ranges from 0 to 2,147,483,647. **always:** Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA area. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table. If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF through the **redistribute** command cannot be advertised to the NSSA area. This parameter is generally used when a router in the NSSA area acts both as the ASBR and the ABR. It prevents external routing information from entering the NSSA area. To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSA) to the NSSA area. **area default-cost** is used on an ABR or ASBR connected to the NSSA area. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1. If an NSSA area has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for converting Type 7 LSAs into Type 5 LSAs. If the current device is always the translator ABR for converting Type 7 LSAs into Type 5 LSAs, use the **translator always** parameter. If the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by **stability-interval**. If the router does not become a translator again during **stability-interval**, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire. In the same NSSA area, it is recommended that **translator always** be configured on only one ABR.

Configuration Example

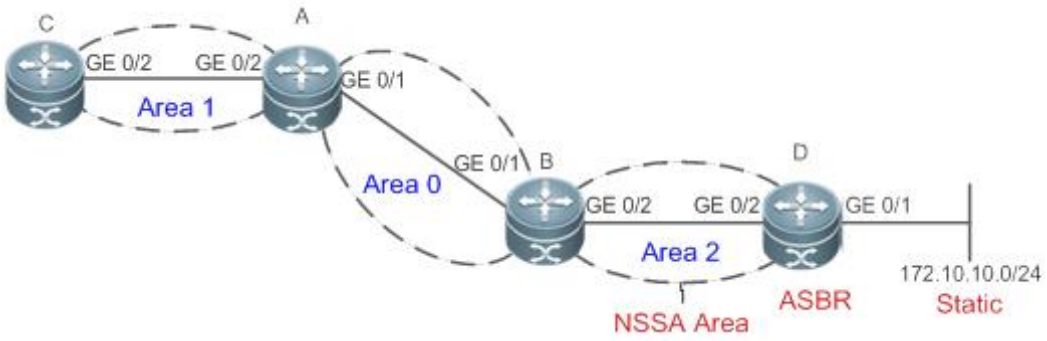
The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring a Stub Area

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.
D	`D# configure terminal` `D(config)#router ospf 1` `D(config-router)# redistribute staticsubnets`
A	`A# configure terminal` `A(config)#router ospf 1` `A(config-router)#area 1 stubno-summary`
C	`C# configure terminal` `C(config)#router ospf 1` `C(config-router)#area 1 stub`
Verification	On Router C, run the **show ip route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Router D.

	C#show ip route ospf O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2

Configuring an NSSA Area

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 2 as the NSSA area on Router B and Router D.
B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 2 nssa
D	D# configure terminal D(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2 D(config)#router ospf 1 D(config-router)#redistribute static subnets D(config-router)#area 2 nssa

Verification	● On Router D, verify that the Type 7 LSA, 172.10.10.0/24, is generated. ● On Router B, verify that Type 5 and Type 7 LSAs coexist on 172.10.10.0/24. ● On Router B, verify that the N-2 route of 172.10.10.0/24 is generated.
D	D# show ip ospf database nssa-external OSPF Router with ID (192.168.6.2) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 61 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8 Length: 36 Network Mask: /24 Metric Type: 2 (Larger than any link state path) TOS: 0 Metric: 20 NSSA: Forward Address: 192.168.6.2 External Route Tag: 0
B	B# show ip ospf database nssa-external OSPF Router with ID (192.168.3.1) (Process ID 1) NSSA-external Link States (Area 0.0.0.1 [NSSA]) LS age: 314 Options: 0x8 (-|-|-|-|N/P|-|-|-) LS Type: AS-NSSA-LSA Link State ID: 172.10.10.0 (External Network Number For NSSA) Advertising Router: 192.168.6.2 LS Seq Number: 80000001 Checksum: 0xc8f8

```
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.6.2
        External Route Tag: 0
B# show ip ospf database external
            OSPF Router with ID (192.168.3.1) (Process ID 1)
                AS External Link States
  LS age: 875
  Options: 0x2 (-|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 172.10.10.0 (External Network Number)
  Advertising Router: 192.168.3.1
  LS Seq Number: 80000001
  Checksum: 0xd0d3
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 192.168.6.2
        External Route Tag: 0


B# show ip route ospf
O N2  172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2
```

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

6.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.
- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table or shield or filter routes.

Configuration Steps

↘ Configuring Inter-Area Route Summarization

- (Optional) This configuration is required when routes of the OSPF area need to be summarized.
- Unless otherwise required, this configuration should be performed on an ABR in the area where routes to be summarized are located.

↘ Configuring External Route Summarization

- (Optional) This configuration is required when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, this configuration should be performed on an ASBR to which routes to be summarized are introduced.

Verification

Run the **show ip route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

↘ Configuring Inter-Area Route Summarization

Command	**area** *area-id***range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
Parameter Description	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The area ID can be a decimal integer or an IP address. *ip-address net-mask*: Defines the network segment of the summarized route. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised. **cost** *cost:* Indicates the metric of the summarized route. The value ranges from 0 to 16777215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an

	area into one route, and advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route. You can configure route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

Command	**summary-address** *ip-address net-mask* [**not-advertise** | **tag** *value*]
Parameter Description	*ip-address*: Indicates the IP address of the summarized route. *net-mask*: Indicates the subnet mask of the summarized route. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised. **tag***value:* Indicates the tag of the summarized route. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPF routing process, each route is advertised to the OSPF routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertised only one summarized route to significantly reduce the size of the routing table. **area range** summarizesthe routes between OSPF routes, whereas **summary-address** summarizes external routes of the OSPF routing domain. When configured on the NSSA ABR translator, **summary-address** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-address** summarizes only redistributed routes.

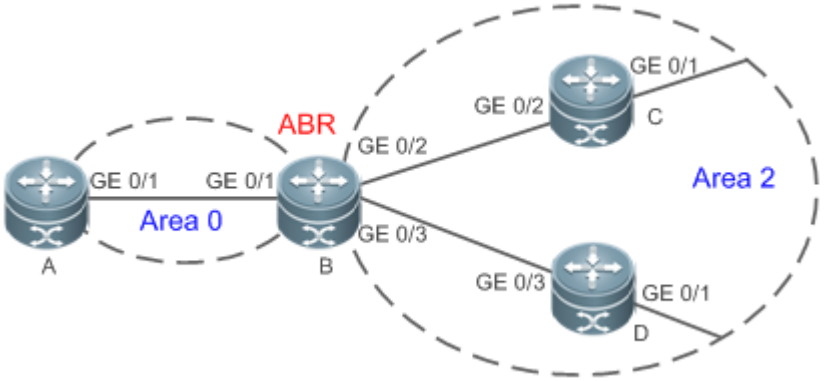
Configuring a Discard Route

Command	**discard-route** { **internal** | **external** }
Parameter Description	**internal:** Indicates that the discard route generated by the **area range** command can be added. **external:** Indicates that the discard route generated by the **summary-address** command can be added.
Command Mode	OSPF routing process configuration mode
Usage Guide	The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table on the

	ABR or ASBR. This route is automatically generated, and is not advertised.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/1 172.16.4.2 D: GE0/2 172.16.3.2 GE0/1 172.16.5.2
Configuration Steps	• Configure the interface IP addresses on all routers. (Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • Summarize routes of area 2 on Router B.
B	`B# configure terminal` `B(config)#router ospf 1` `B(config-router)#area 2 range 172.16.0.0 255.255.0.0`
Verification	On Router A, verify that the entry 172.16.0.0/16 is added to the routing table.
A	`A#show ip route ospf` `O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1`

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

6.4.6 Configuring Route Filtering

Configuration Effect

- Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Steps

↘ Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users should be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, this configuration should be performed on an ABR in the area where filtered routes are located.

↘ Configuring Redistributed Route Filtering

- (Optional) This configuration is required if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, this configuration should be performed on an ASBR to which filtered routes are introduced.

↘ Configuring Learned Route Filtering

- (Optional) This configuration is required if users should be restricted from accessing a specified destination network.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

↘ Configuring a Passive Interface

Command	**passive-interface**{ **default** | *interface-type interface-number* | *interface-type interface-numberip-address*}
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interface will be configured as passive interfaces.

	interface-type interface-numberip-address: Specifies an address of the interface as the passive address.
Command Mode	OSPF routing process configuration mode
Usage Guide	To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address.

Configuring the LSA Update Packet Filtering

Command	**ip ospf database-filter all out**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function on an interface to prevent sending the LSA update packet on this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up the adjacency with neighbors and receives LSAs from neighbors.

Configuring Inter-Area Route Filtering

Command	**area***area-id***filter-list** {**access***acl-name*| **prefix** *prefix-name*} {**in** | **out**}
Parameter Description	*area-id*: Indicates the area ID. **access** *acl-name*: Indicates the associated ACL. **prefix** *prefix-name*: Indicates the associated prefix list. **in** | **out:** Filters routes that are received by or sent from the area.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be configured only on an ABR. Use this command when it is required to configure filtering conditions for inter-area routes on the ABR.

Configuring Redistributed Route Filtering

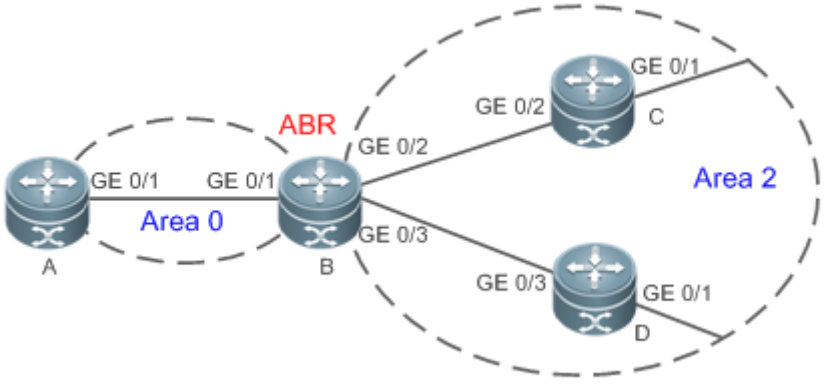
Command	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected ospf** *process-id* **| rip | static**]
Parameter Description	*access-list-number* | *name*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefixlist for filtering. **connected | ospf** *process-id* | **rip** | **static**: Indicates the source of routes to be filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPF. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and the prefixlist filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefixlist cannot be configured to filter the same routes.

Configuring Learned Route Filtering

Command	**distribute-list** {[*access-list-number* | *name*] | **prefix***prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* } **in** [*interface-typeinterface-number*]
Parameter Description	*access-list-number* | *name*: Uses the ACL for filtering. **gateway***prefix-list-name*: Uses the gateway for filtering. **prefix***prefix-list-name*: Uses the prefixlist for filtering. **route-map** *route-map-name:* Uses the route map for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL, prefix list, and route map filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes of a specified interface, the prefix list or router map cannot be configured for filtering routes of the same interface.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.

A	A# configure terminal A(config)#access-list 3 permit host 172.16.5.0 A(config)#router ospf 1 A(config-router)#distribute-list 3 in GigabitEthernet 0/1
Verification	● On Router A, check the routing table. Verify that only the entry 172.16.5.0/24 is loaded.
A	A# show ip route ospf O 172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated.

6.4.7 Modifying Route Cost and AD

Configuration Effect

- Change the OSPF routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- The OSPF basic functions must be configured.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Steps

↘ Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

↘ Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

Configuring the Default Metric for Redistribution

- Optional.
- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- This configuration is mandatory if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ip ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ip route** command to verify that the costs of external routes introduced to the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-costreference-bandwidth** *ref-bw*
Parameter Description	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.
Command Mode	OSPF routing process configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of an Interface

Command	**ip ospf cost***cost*
Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area***area-id* **default-cost***cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area. An ABR in a stub area or an ABR/ASBR in an NSSA area is allowed to advertise an LSA indicating the default route in the stub or NSSA area. You can run the **area default-cost** command to modify the cost of the advertised LSA.

Configuring the Default Metric for Redistribution

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric**command must be used together with the **redistribute**command to modify the initial metrics of all redistributed routes. The **default-metric**command does not take effect on external routes that are injected to the OSPF routing domain by the **default-information originate** command.

Configuring the Maximum Metric

Command	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup**[*seconds*]] [**summary-lsa** [*max-metric-value*]]
Parameter Description	**router-lsa**: Sets the metrics of non-stub links in the Router LSA to the maximum value (0xFFFF). **external-lsa**: Allows a router to replace the metrics of external LSAs (including Type 5 and Type 7 LSAs) with the maximum metric. *max-metric-value*: Indicates the maximum metric of the LSA. The default value is 16711680. The value ranges from 1 to 16,777,215. **include-stub:** Sets the metrics of stub links in the Router LSA advertised by the router to the maximum value. **on-startup:** Allows a router to advertises the maximum metric when started. *seconds:* Indicates the interval at which the maximum metric is advertised. The default value is 600s. The value ranges from 5 to 86,400. **summary-lsa:** Allows a router to replace the metrics of summary LSAs (including Type 3 and Type 4 LSAs) with the maximum metric.
Command Mode	OSPF routing process configuration mode
Usage Guide	After the **max-metric router-lsa** command is executed, the metrics of the non-stub links in the Router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored. By default, if the **max-metric router-lsa** command is executed, the stub links still advertise common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric. If an ABR does not wish to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the Summary LSA to the maximum metric. If an ASBR does not wish to transfer external traffic, use the **external-lsa** parameter to set the metric of the external LSA to the maximum metric. The **max-metric router-lsa** command is generally used in the following scenarios: Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. ● Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic. ● Delete a device gracefully from the network. After the **max-metric router-lsa** command is executed, the current device advertises the maximum metric among all metrics of routes. In this way, other devices on the network can select the standby path for data transmission before the device is shut down. In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

Configuring RFC1583Compatibility

Command	**compatible rfc1583**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibilityis configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibilityis not configured, a path in a non-backbone area is preferentially selected.

Configuring the AD

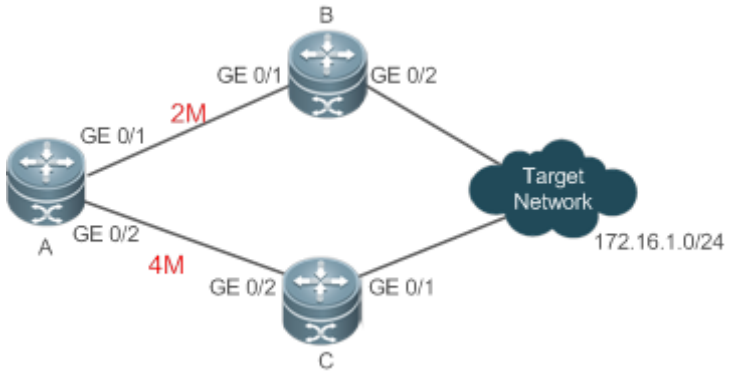
Command	**distance** { *distance* | **ospf** { [**intra-area***distance*] [**inter-area***distance*][**external** *distance*]} }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area** *distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	Use this command to specify different ADs for different types of OSPF routes.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring the Cost of an Interface

Scenario



Remarks	The interface IP addresses are as follows: A: GE0/1 192.168.1.1 GE0/2 192.168.2.1 B: GE0/1 192.168.1.2 GE0/2 192.168.3.2 C: GE0/1 192.168.4.2 GE0/2 192.168.2.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf cost 10 A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
Verification	On Router A, check the routing table. The next hop of the optimum path to 172.16.1.0/24 is Router B.
A	A# show ip route ospf O E2172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ip ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

6.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

Configuration Steps

↘ Configuring the Authentication Type of an Area

- (Optional) This configuration is recommended if the same authentication type should be used on all interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

Configuring the Authentication Type of an Interface

- (Optional) This configuration is recommended if the different authentication types should be used on different interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

Configuring a Plain Text Authentication Key for an Interface

- Optional.
- This configuration is required if a router accesses a network that requires plain text authentication.

Configuring an MD5 Authentication Key for an Interface

- (Optional) MD5 authentication features a high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication.
- This configuration is required if a router accesses a network that requires MD5 authentication.

Verification

- If routers are configured with different authentication keys, run the **show ip ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ip ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring the Authentication Type of an Area

Command	**area** *area-id***authentication** [**message-digest**]
Parameter Description	*area-id*: Indicatesthe ID of the area where OSPF authentication is enabled. The area ID can be a decimal integer or an IP address. **message-digest**: Enables MD5 authentication.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports three authentication types: (1) Type 0: No authentication is required. If this command is not configured to enable OSPF authentication, the authentication type in the OSPF data packet is 0. (2) Type 1: The authentication type is plain text authentication if this command is configured but does not contain the **message-digest** parameter. (3) Type 3: The authentication type is MD5 authentication if this command is configured and contains the **message-digest** parameter. All routers in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors. You can run the interface configuration command **ip ospf authentication-key** to configure the plain text authentication key, or **ip ospf message-digest-key** to configure the MD5 authentication key.

Configuring the Authentication Type of an Interface

Command	**ip ospfauthentication** [**message-digest** | **null**]
Parameter Description	**message-digest**: Indicates that MD5 authentication is enabled on the current interface. **null**: Indicates that authentication is disabled.
Command Mode	Interface configuration mode
Usage Guide	If the **ip ospfauthentication** command does not contain any option, it indicates that plain text authentication is enabled. If you use the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to null, authentication is disabled forcibly.When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

Configuring a Plain Text Authentication Key for an Interface

Command	**ip ospf authentication-key**[**0** |**7**]*key*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key*: Indicates the key. The key is a string of up to eight characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf authentication-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. You can enable or disable authentication in an OSPF area by running the **areaauthentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

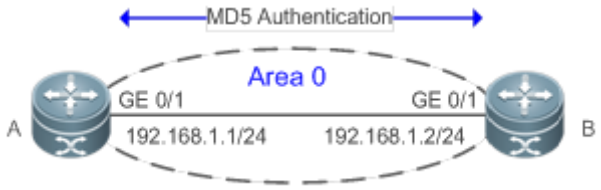
Configuring an MD5 Authentication Key for an Interface

Command	**ip ospf message-digest-key** *key-id* **md5**[**0** |**7**]*key*
Parameter Description	*key-id:* Indicates the key ID. The value ranges from 1 to 255. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key:* Indicates the key. The key is a string of up to 16 characters.
Command Mode	Interface configuration mode

Usage Guide	The key configured by the **ip ospf message-digest-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. The same key ID on neighbor routers must correspond to the same key. You can enable or disable authentication in an OSPF area by running the **area authentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially. The RGOS software supports smooth modification of the MD5 authentication key. A new MD5 authentication key must be first added before the old key can be deleted. When an OSPF MD5 authentication key is added to a router, the router determines that other routers do not use the new key yet and therefore uses different keys to send multiple OSPF packets until it confirms that the new key has been configured on neighbors. After configuring the new key all routers, you can delete the old key.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.
A	`A# configure terminal` `A(config)#router ospf 1` `A(config-router)#area 0 authentication message-digest` `A(config-router)#exit` `A(config)#interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello`

B	B# configure terminal B(config)#router ospf 1 B(config-router)#area 0 authentication message-digest B(config-router)#exit B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello
Verification	On Router A and Router B, verify that the OSPF neighbor status is correct.
A	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:32 192.168.1.2 GigabitEthernet 0/1
B	A#show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/DR 00:00:32 192.168.1.1 GigabitEthernet 0/1

Common Errors

- The authentication modes configured on routers are inconsistent.
- The authentication keys configured on routers are inconsistent.

6.4.9 Enabling Overflow

Configuration Effect

- New routes are not loaded to routers when the router memory is insufficient.
- New routes are not loaded to routers when the usage of the database space reaches the upper limit.

Notes

- The OSPF basic functions must be configured.
- After a router enters the overflow state, you can run the **clear ip ospf process** command, or stop and then restart the OSPF to exit the overflow state.

Configuration Steps

↘ **Configuring the Memory Overflow Function**

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the Database Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the External LSA Database Overflow Function

- Optional.
- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.

Verification

- After the memory becomes insufficient, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.
- After the usage of the database space reaches the upper limit, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.

Related Commands

Configuring the Memory Overflow Function

Command	**overflow memory-lack**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively ensure that the memory usage does not increase. After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the occurrence probability of this problem, OSPF generates a default route to the null interface, and this route always exists in the overflow state. You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state. You can use the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

Configuring the Database Overflow Function

Command	**overflow database***number* [**hard	soft**]
Parameter Description	*number*: Indicates the maximum number of LSAs. The value ranges from 1 to 4,294,967,294. **hard**: Indicates that the OSPF process will be stopped if the number of LSAs exceeds the limit. **soft:** Indicates that a warning will be generated if the number of LSAs exceeds the limit.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs exceeds the limit, use the **hard** parameter if the OSPF process should be stopped, and use the **soft** parameter if a warning should be generated without stopping the OSPF process.

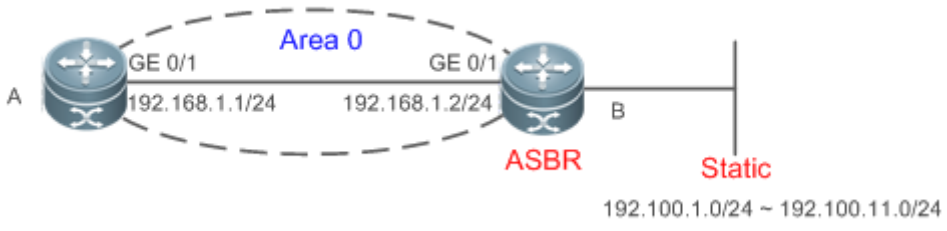
Configuring the External LSA Database Overflow Function

Command	**overflow database external** *max-dbsize wait-time*
Parameter Description	*max-dbsize*: Indicates the maximum number of external LSAs. This value must be the same on all routers in the same AS. The value ranges from 0 to 2,147,483,647. *wait-time*: Indicates the waiting time after a router in overflow state attempts to restore the normal state. The value ranges from 0 to 2,147,483,647.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the number of external LSAs of a router exceeds the configured **max-dbsize**, the router enters the overflow state. In this state, the router no longer loads external LSAs and deletes external LSAs that are generated locally. After *wait-time* elapses, the device restores the normal state, and loads external LSAs again. When using the overflow function, ensure that the same **max-dbsize** is configured on all routers in the OSPF backbone area and common areas; otherwise, the following problems may occur: Inconsistent LSDBs throughout network are inconsistent, and the failure to achieve the full adjacency Incorrect routes, including routing loops Frequent retransmission of AS external LSAs

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring the External LSA Database Overflow Function

Scenario	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router B, configure redistribution and introduce external static routes. ● On Router B, configure the maximum number of external LSAs.
B	B# configure terminal B(config)# router ospf 1 B(config-router)# redistribute static subnets
A	A# configure terminal A(config)# router ospf 1 A(config-router)# overflow database external 10 3
Verification	On Router B, configure 11 static routes (192.100.1.0/24 to 192.100.11.0/24). On Router A, verify that only 10 static routes are loaded.
A	A# show ip route ospf O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1 O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- The OSPF adjacency is abnormal because the maximum number of LSAs is inconsistent on different routers.

6.4.10 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacencymore quickly when a router is connected with a lot of other routers.
- This configuration is performed on a core router.

Verification

- Run the **show ip ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which one OSPF process can concurrently initiates or accepts interaction.

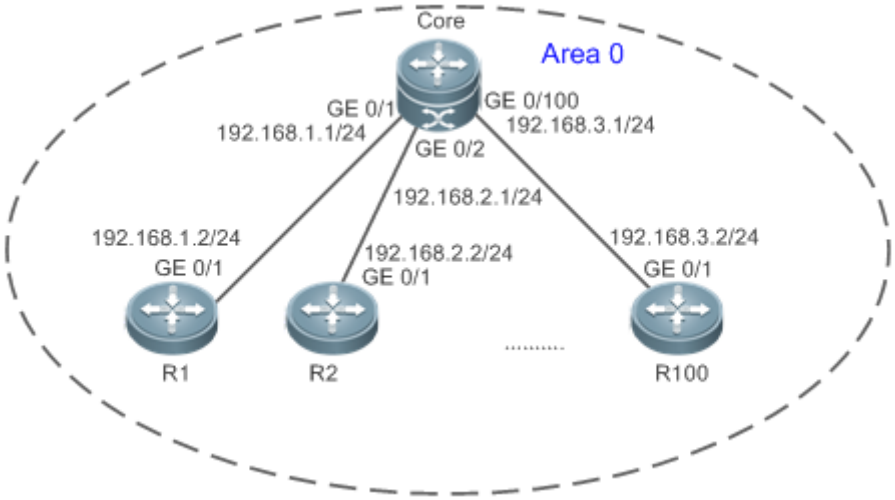
Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**router ospf max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the router Core, set the maximum number of concurrent neighbors to 4.
Core	`Core# configure terminal` `Core(config)# router ospf max-concurrent-dd 4`
Verification	On therouter Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

6.4.11 Disabling Source Address Verification

Configuration Effect

- The unicast routing service can be provided even if the interface IP addresses of neighbor routers are not in the same network segment.

Notes

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

Configuration Steps

Disabling Source Address Verification

- (Optional) This configuration is mandatory if an adjacency should be set up between routers with interface IP addresses in different network segments.
- This configuration is performed on routers with interface IP addresses in different network segments.

Verification

- An adjacency can be set up between routers in different network segments.

Related Commands

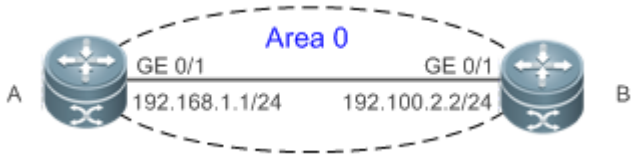
Disabling Source Address Verification

Command	**ip ospf source-check-ignore**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In some scenarios, the source address may not meet the preceding requirement, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Disabling Source Address Verification

Scenario	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the network types of interfaces on all routers to P2P. ● Disable source address verification on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
Verification	On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.100.2.2 1 Full/- 00:00:34 192.100.2.2 GigabitEthernet 0/1

6.4.12 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

Verification

The adjacency can be set up between routers with different MTUs.

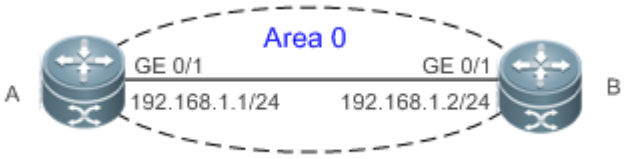
Related Commands

Disabling MTU Verification

Command	ip ospf mtu-ignore
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	• Configure the interface IP addresses on all routers. (Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • Configure different MTUs for interfaces on two routers. • Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1400 A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore

B	B# configure terminal B(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip mtu 1600 B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore
Verification	● On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:34 192.168.1.2 GigabitEthernet 0/1

6.4.13 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Non-Hello packets can also be used to maintain the adjacency.

Related Commands

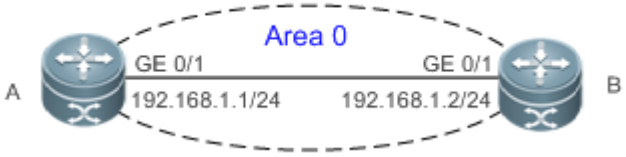
↘ Enabling Two-Way Maintenance

Command	**two-way-maintain**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead

	interval, the adjacency will be destroyed due to timeout. If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)
A	A# configure terminal A(config)#routerospf 1 A(config-router)#two-way-maintain
Verification	When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/BDR 00:00:40 192.168.1.2 GigabitEthernet 0/1

6.4.14 Enabling GR

Configuration Effect

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Related Commands

Configuring the OSPF GR Function

Command	**graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations. Run the**graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains

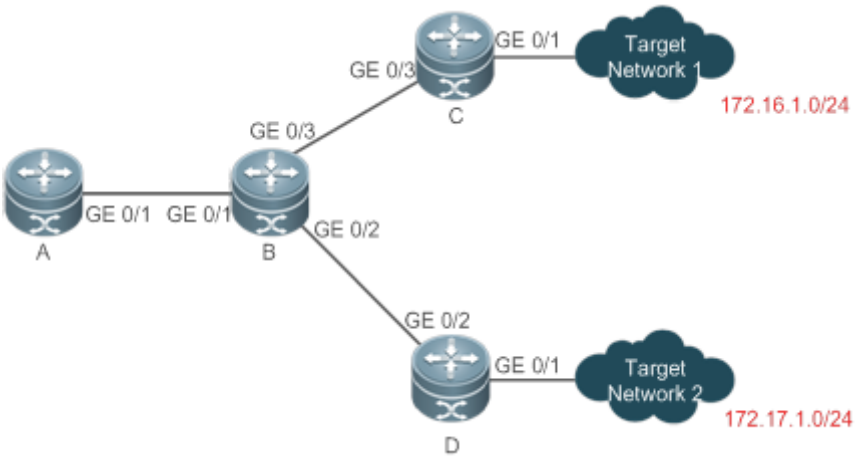
	stable.If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. Disabling topology detection: If OSPF cannot converge in time when thetopology changes during the hot standby process, forwarding black-hole may appear in a long time. Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appearin a long time. This can minimize the forwarding interruption time during the hot standby process.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable | strict-lsa-checking | internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR. After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

<table>
<tr><td>Scenario</td><td>


<table>
<tr><td>Remarks</td><td>The interface IP addresses are as follows:
A: GE 0/1 192.168.1.1
B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1
C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2
D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2</td></tr>
</table>
</td></tr>
<tr><td>Configuration Steps</td><td>

Configure the interface IP addresses on all routers. (Omitted)
Configure the OSPF basic functions on all routers. (Omitted)
On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.)
On Router B, enable the GR function.

</td></tr>
<tr><td>B</td><td>
<pre>B# configure terminal
B(config)# router ospf1
B(config-router)# graceful-restart</pre>
</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Verification</td><td>

Trigger a hot standby switchover on Router B, and verify that the routing tables of destination networks 1 and 2 remain unchanged on Router A during the switchover.
Trigger a hot standby switchover on Router B, ping destination network 1 from Router A, and verify that data forwarding is not interrupted during the switchover.

</td></tr>
</table>

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

6.4.15 Configuring the Network Management Function

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP-Server before enabling the OSPF MIB function.
- You must enable the Trap function of the SNMP-Server before enabling the OSPF Trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

Configuration Steps

↘ Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- This configuration is performed on all routers.

↘ Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.
- This configuration is performed on all routers.

↘ Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- This configuration is performed on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

↘ Binding the MIB with the OSPF Process

Command	**enable mib-binding**
Parameter Description	N/A
Command	OSPF routing process configuration mode

Mode	
Usage Guide	The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP. By default, the OSPFv2 MIB is bound with the OSPFv2 process with the smallest process ID, and all user operations take effect on this process. If you wish to perform operations on a specified OSPFv2 through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

Command	**enable traps**[**error** [**IfAuthFailure | IfConfigError | IfRxBadPacket | VirtIfAuthFailure | VirtIfConfigError | VirtIfRxBadPacket**] | **lsa** [**LsdbApproachOverflow | LsdbOverflow | MaxAgeLsa | OriginateLsa**] | **retransmit** [**IfTxRetransmit | VirtIfTxRetransmit**] | **state-change**[**IfStateChange | NbrRestartHelperStatusChange | NbrStateChange | NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange | VirtNbrRestartHelperStatusChange| VirtNbrStateChange**]]
Parameter Description	**IfAuthFailure**: Indicates that an interface authentication failure occurs. **IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfAuthFailure:** Indicates that a virtual interface authentication failure occurs. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **LsdbApproachOverflow:** Indicates that the number of external LSAs has reached 90% of the upper limit. **LsdbOverflow:** Indicates that the number of external LSAs has reached the upper limit. **MaxAgeLsa:** Indicates that the LSA aging timer expires. **OriginateLsa:** Indicates that a new LSA is generated. **IfTxRetransmit:** Indicates that a packet is retransmitted on the interface. **VirtIfTxRetransmit:** Indicates that a packet is retransmitted on the virtual interface. **IfStateChange:** Indicates that interface state changes. **NbrRestartHelperStatusChange:**Indicates that the state of the neighbor GR process changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes.
Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled

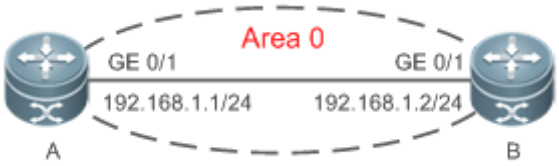
	concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.
A	A# configure terminal A(config)# snmp-server host 192.168.2.2 traps version 2c public A(config)# snmp-server community public rw A(config)# snmp-server enable traps A(config)# router ospf 10 A(config-router)# enable mib-binding A(config-router)# enable traps
Verification	Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

Configurations on the SNMP-Server are incorrect. For example, the MIB or trap function is not enabled.

6.4.16 Modifying Protocol Control Parameters

Configuration Effect

Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

Configuring the Hello Interval

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on routers at both end of a link.

Configuring the Dead Interval

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- This configuration is performed on routers at both end of a link.

Configuring LSU Retransmission Interval

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

Configuring the LSA Generation Time

- (Optional) You are advised to retain the default configuration.

Configuring the LSA Group Refresh Time

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- This configuration is performed on an ASBR or ABR.

Configuring LSA Repeated Receiving Delay

- (Optional) You are advised to retain the default configuration.

Configuring the SPF Computation Delay

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.

- This configuration is performed on all routers.

Configuring the External Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Run the **show ip ospf**and**show ip ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ip ospf hello-interval***seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the Hello interval.

Configuring the Dead Interval

Command	**ip ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ip ospf transmit-delay***seconds*
Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command	Interface configuration mode

Mode	
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmit and line propagation delays on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command. If the value of the Age field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring LSU Retransmission Interval

Command	**ip ospf retransmit-interval***seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 0 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.
Command Mode	Interface configuration mode
Usage Guide	After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a high convergence requirement is raised when a link changes, you can set **delay-time** to a smaller value. You can also appropriately increase values of the preceding parameters to reduce the CPU usage. When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacinglsa-group** *seconds*
Parameter	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.

Description	
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. In order to use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole. If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs processes upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 1000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 1,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs is large and the device load is heavy in an environment, properly configuring **transimit-time** and **transimit-count** can limit the number of LS-UPD packets flooded on a network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of **transimit-time** and increasing the value of **transimit-count** can accelerate the environment convergence.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival** *arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the Inter-Area Route Computation Delay

Command	**timers throttle route inter-area** *ia-delay*
Parameter Description	*ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode

Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the External Route Computation Delay

Command	**timers throttle route ase** *ase-delay*
Parameter Description	*ase-delay*: Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the SPF Computation Delay

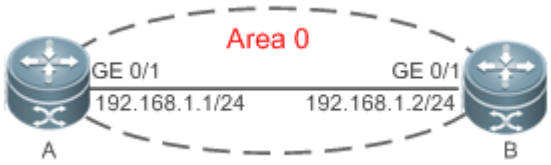
Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses. *spf-holdtime*: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: indicates the metric of the summarized route.
Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-dela**y and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers**

	throttle spf prevail.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 6.4.1 "Configuring OSPF Basic Functions."

Configuring the Hello Interval and Dead Interval

Scenario	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15 A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50
Verification	Check the interface parameters on Router A. Verify that the Hello interval is 10s and the dead interval is 50s.

A	A# show ip ospf interface GigabitEthernet 0/1 is up, line protocol is up Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500 Matching network config: 192.168.1.0/24 Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 0 Crypt Sequence Number is 4787 Hello received 465 sent 466, DD received 8 sent 8 LS-Req received 2 sent 2, LS-Upd received 8 sent 21 LS-Ack received 14 sent 7, Discarded 3

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

6.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears and resets an OSPF process.	**clear ip ospf** [*process-id*] **process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ip ospf** [*process-id*]
Displays the OSPF internal routing table, including routes to ABRs and ASBRs.	**show ip ospf**[*process-id*] **border-routers**
Displays information about the OSPF LSDB.	**show ip ospf** [*process-id area-id*] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }][{ **adv-router** *ip-address*| **self-originate** } |*link-state-id* | **brief**][**database-summary** | **max-age** | **detail**]

Description	Command
Displays OSPF-enabled interfaces.	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Displays the OSPF neighbor list.	**show ip ospf** [*process-id*] **neighbor** [**detail**] [*interface-typeinterface-number*] [*neighbor-id*]
Displays the OSPF routing table.	**show ip ospf** [*process-id*] **route**[**count**]
Displays the number of times SPT is computed in the OSPF area.	**show ip ospf** [*process-id*] **spf**
Displays the summarized route of OSPF redistributed routes.	**show ip ospf**[*process-id*] **summary-address**
Displays the OSPF network topology information.	**show ip ospf** [*process-id*[*area-id*]] **topology**[**adv-router***adv-router-id* [*router-id*] | **self-originate**[*router-id*]]
Displays OSPF virtual links.	**show ip ospf** [*process-id*] **virtual-links** [*ip-address*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs OSPF events.	**debug ip ospf events** [**abr**|**asbr**|**lsa**|**nssa**|**os**|**restart**| **router**|**slink**| **vlink**]
Debugs OSPF interfaces.	**debug ip ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ip ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ip ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ip ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ip ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ip ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

7 Configuring OSPFv3

7.1 Overview

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that is used within the Autonomous System (AS) to allow routers to obtain a route to a remote network.

OSPF Version 2 (OSPFv2) is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, notifications can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be L3 switches, routers, or firewall.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv3.

Protocols and Standards

RFC2740	This document describes the modifications to OSPF to support version 6 of the Internet Protocol (IPv6).
draft-ietf-ospf-ospfv3-graceful-restart	This document describes the OSPFv3 graceful restart. The OSPFv3 graceful restart is identical to OSPFv2 except for the differences described in this document. These differences include the format of the grace Link State Advertisements (LSA) and other considerations.
draft-ietf-ospf-ospfv3-mib-11	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based internets. In particular, it defines objects for managing the Open Shortest Path First Routing Protocol for IPv6.

7.2 Applications

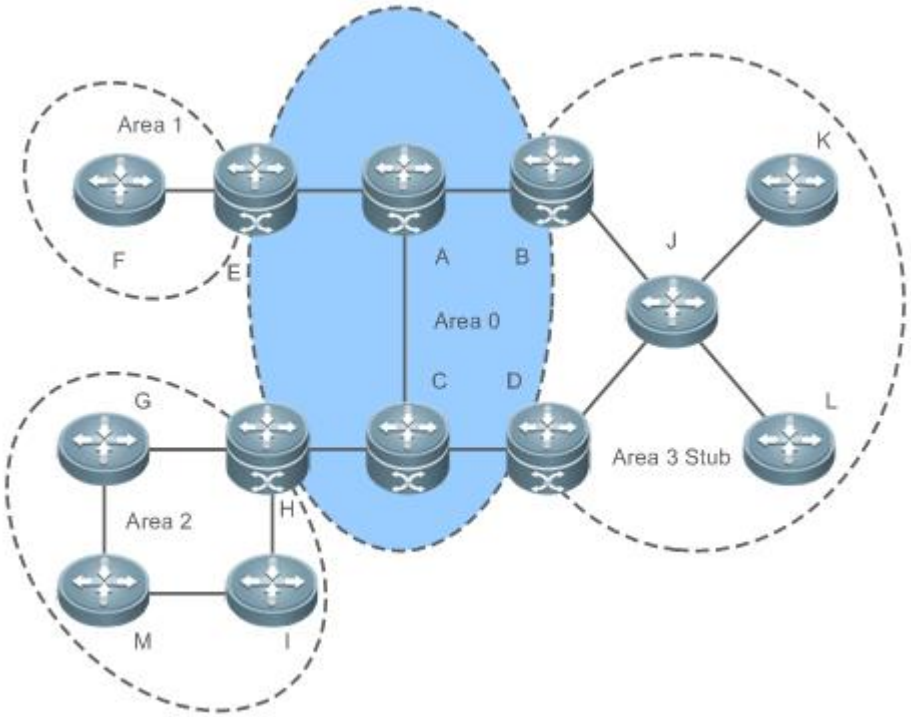
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.

7.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal area located on the stub be configured as a stub area. As shown in Figure 7-1, the network is divided into four areas. Communication between these areas must go through the backbone area, that is, area 0.

Figure 7-1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

7.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, an AS is also called a routing domain.
An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

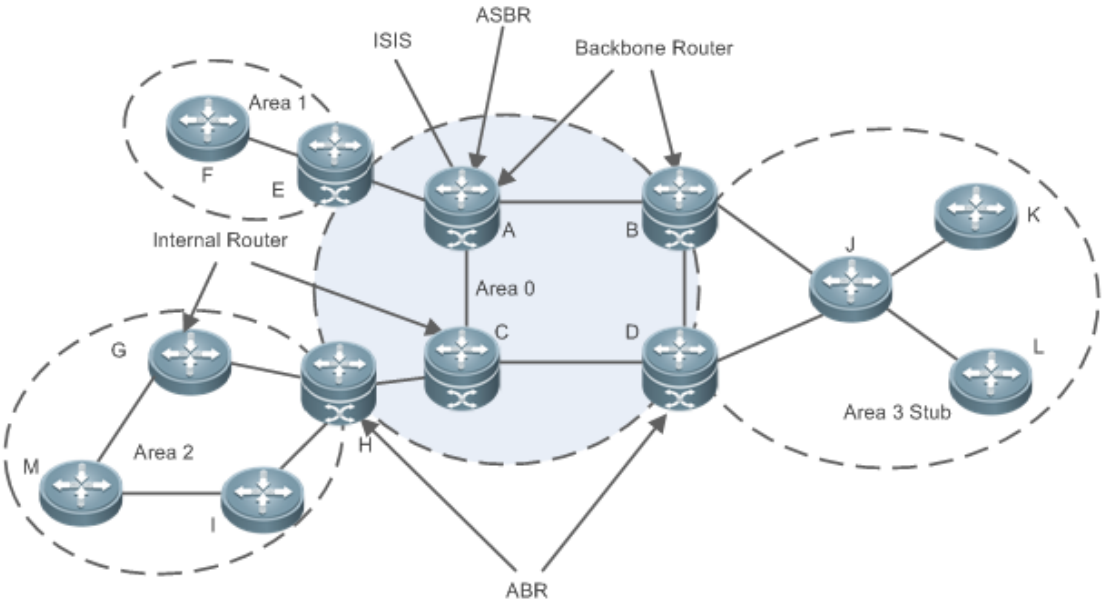
OSPF supports multiple instances, and each instance corresponds to an OSPF process.
One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.
An OSPF packet header contains the Instance ID field, and multiple OSPF instances can run concurrently on a single link. The process ID is valid only on the local device.

RouterID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.
If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.
An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.
Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.
Figure 7-2Division of the OSPF Areas



OSPF Router

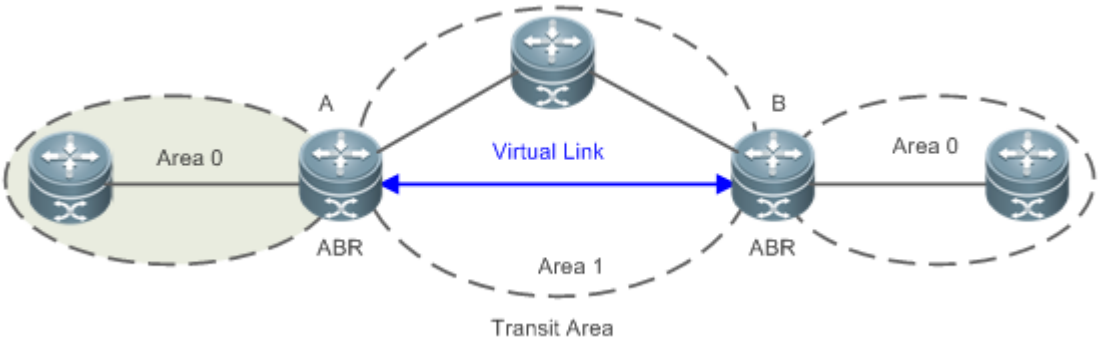
The following types of routers are defined in OSPF, and assigned with different responsibilities:

- Internal router
  All interface of an interval router belong to the same OSPF area. As shown in Figure 7-2, A, C, F, G, I, M, J, K, and L are internal routers.
- Area border router (ABR)
  An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. As shown in Figure 7-2, B, D, E, and H are ABRs.
- Backbone router
  A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers. As shown in Figure 7-2, A, B, C, D, E, and H are backbone routers.
- AS boundary router (ASBR)
  An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. As shown in Figure 7-2, A is an ASBR.

Virtual Link

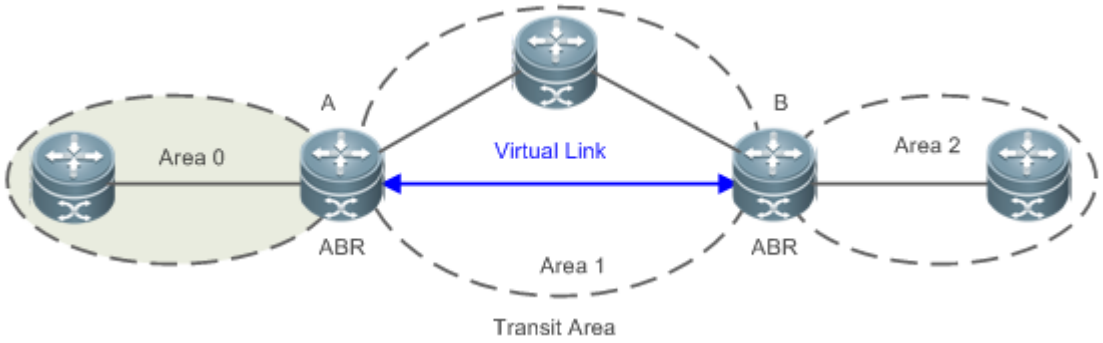
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 7-3Discontinuous Backbone Area on the Physical Network



As shown in Figure 7-3, a virtual link is set up between A and B to connect two separated parts of Area 0. Area 1 is a transit area, and A and B are ABRs of Area 1.

Figure 7-4Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 7-4, a virtual link is set up between A and B to extend Area 0 to B so that Area 0 can be directly connected to Area 2 on B. Area 1 is a transit area, A is an ABR of Area 1, and B is an ABR of Area 0 and Area 2.

LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA(Type2)	This LSA is originated by a designated router (DR). It describes the state of the current link, and is advertised only within the area where the DR is located.
Inter-Area-Prefix-LSA(Type3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas or Not-So-Stubby Area (NSSA) areas.
Inter-Area-Router-LSA(Type4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except areas where the ASBR is located.
AS-external-LSA(Type5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
Link-LSA(Type8)	This LSA is originated by every router. It describes the link-local address and IPv6 prefix address of each link, and provides the link option that will be set in the

LSA Type	Description
	Network-LSA. It advertised only on the current link.
Intra-Area-Prefix-LSA(Type9)	Every router or DR generates one or more Intra-Area-Prefix-LSAs, which are advertised in the area to which the router or DR belongs. ● The Intra-Area-Prefix-LSA generated by a router describes the IPv6 prefix address associated with the Route-LSA. ● The Intra-Area-Prefix-LSA generated by a DR describes the IPv6 prefix address associated with the Network-LSA.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Properly plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.
Enhanced Security and Reliability	Use functions such as authentication and BFD correlation to enhance security, stability, and reliability of OSPF.
Network Management Functions	Use functions such as the MIB and Syslog to facilitate OSPF management.

7.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
  An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
  A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- Shortest Path Tree (SPT) computation → Formation of a routing table
  The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

Working Principle

Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Instance ID of the originating router interface (or virtual link)
- Interface ID of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- Hello interval of the originating router interface (or virtual link)
- Neighbor dead interval of the originating router interface (or virtual link)
- IP addresses of the DR and Backup Designated Router (BDR)
- Router ID of the neighbor of the originating router

Database Synchronization → Full Adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.
- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

OSPF will be very quiet without changes in link costs or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

SPT Computation → Formation of a Routing Table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

OSPF Network Types

A router does not necessarily need to exchange LSAs with every neighbor and set up an adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency:

- Broadcast

  Neighbors are discovered, and the DR and BDR are elected.

  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.

  Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.

- Non-broadcast multiple access (NBMA)

  Neighbors are manually configured, and the DR and BDR are elected.

  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.

  X.25, frame relay, and ATM belong to NBMA networks by default.

- Point-to-point (P2P)

  Neighbors are automatically discovered, and the DR or BDR is not elected.

  LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.

  PPP, HDLC, and LAPB belong to the P2P network type by default.

- Point-to-multipoint(P2MP)

  Neighbors are automatically discovered, and the DR or BDR is not elected.

  LSAs are exchanged between any two routers, and the adjacency is set up.

  Networks without any link layer protocol belong to the P2MP network type by default.

- P2MP broadcast

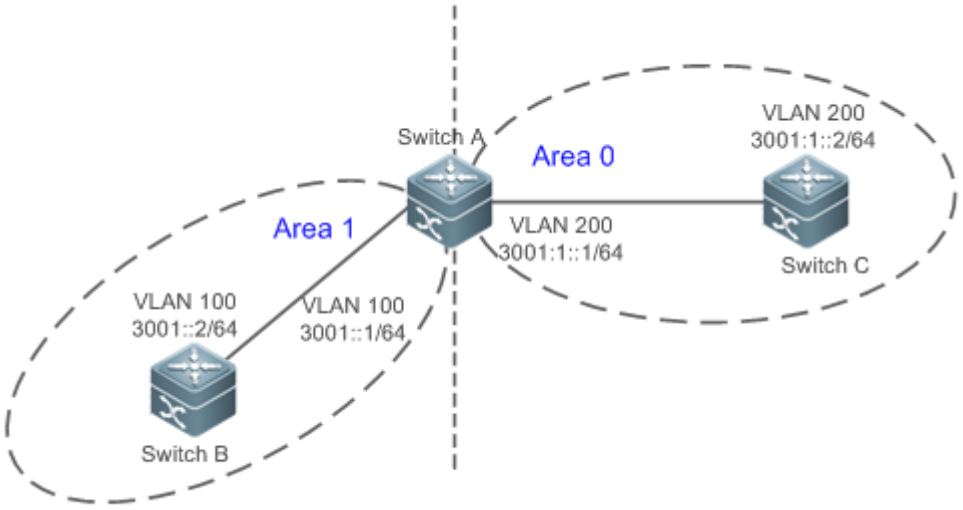
  Neighbors are manually configured, and the DR or BDR is not elected.

  LSAs are exchanged between any two routers, and the adjacency is set up.

  Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 7-5



Display the OSPF routes (marked in red) in the routing table of Router C.

```
C#show ipv6 route ospf

IPv6 routing table name is Default(0) global scope - 7 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

      O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1, OE2 - OSPF external
type 2

      ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2

      [*] - NOT in hardware forwarding table


L     ::1/128  via Loopback, local host

OI    3001::/64  [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200

C     3001:1::/64  via VLAN 200, directly connected

L     3001:1::2/128  via VLAN 200, local host

L     FE80::/10  via ::1, Null0

C     FE80::/64  via VLAN 200, directly connected

L     FE80::21A:A9FF:FE01:FB1F/128  via VLAN 200, local host
```

A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Intra-area route

  This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OI: Inter-area route

  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- OE1: Type 1 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- OE2: Type 2 external route

  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.

- ON1: Type 1 external route of the NSSA area

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

- ON2: Type 2 external route of the NSSA area

  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

Reliability of OE2 and ON2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **ipv6 router ospf** 1 command to create an OSPF process on the router.

Run the **ipv6 ospfarea** command to enable OSPF on an interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IPv4 address among the IPv4 addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IPv4 addresses are not available, the OSPF process elects the largest IPv4 address among the IPv4 addresses of all the physical ports as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ipv6 ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).
Run the **ipv6 ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.
Use the **poll-interval** parameter in the **ipv6 ospf neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.
Run the **ipv6 ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.
Run the **ipv6 ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.
Use the **hello-interval** parameter in the **area virtual-link** command to modify the Hello interval on the virtual link. The default value is 10s.
Use the **dead-interval** parameter in the **area virtual-link** command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.
Use the **transmit-delay** parameter in the **area virtual-link** command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.
Use the **retransmit-interval** parameter in the **area virtual-link** command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.
Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.
Run the **timers pacing lsa-group** command to modify the LSA group update interval. The default value is 30s.
Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.
Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.
Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

↘ OSPF Network Types

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.
Run the **ipv6 ospf network** command to manually specify the network type of an interface.
Run the **ipv6 ospf neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.
Run the **ipv6 ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

7.3.2 OSPF Route Management

Properly plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

(Totally) Stub Area and (Totally) NSSA Area

The (totally) stub and (totally) NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type 1 and Type 2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA area	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

The ABR uses Type 3 LSAs to advertise a default route to the (totally) stub or NSSA area.

The ABR converts Type 7 LSAs in the totally NSSA area to Type 5 LSAs, and advertise Type 5 LSAs to the backbone area.

- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of OE1, OE2, and OI routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area OI: a route to a destination network in another area OE1 or OE2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area OI: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area OI: a default route
NSSA area	O: a route to a destination network in the local area OI: a route or a default route to a destination network in another area ON1 or ON2: a route or default route to a destination network segment outside the AS (via an ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area OI: a default route ON1 or ON2: a route or default route to a destination network segment outside the AS

Area	Routes Available in the Routing Table of a Router Inside the Area
	(via an ASBR in the local area)

Route Redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.
Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

Default Route Introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.
Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.
By default, the ABR advertises inter-area routing information by using Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs.If continuous network segments exist, it is recommended that you configure route summarization.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.
Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path.The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

Using configuration commands, you can modify the following link costs:

- Cost from an interface to a directly connected network segment and cost from the interface to a neighbor
- Cost from an ABR to the default network segment
- Cost from an ASBR to an external network segment and cost from the ASBR to the default network segment

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Route Source	Directly-connected network	Static route	EBGP Route	OSPF Route	IS-IS Route	RIP Route	IBGP Route	Unreachable Route
Default AD	0	1	20	110	115	120	200	255

Related Configuration

Stub Area

By default, no stub or NSSA area is configured.

Run the **area stub** command to configure a specified area as a stub area.

A backbone area cannot be configured as a stub area.

A transit area (with virtual links going through) cannot be configured as a stub area.

An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce a default route.

After configuring route redistribution and default route introduction, the router automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **area range** command to summarize routes (Type 3 LSA) distributed between areas on the ABR.

Run the **summary-prefix** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
  The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
  Run the **auto-cost reference-bandwidth** command to set the reference bandwidth of the auto cost. The default value is 100 Mbps.
  Run the **ipv6 ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
  The default value is the auto cost.
  Use the **cost** parameter in the **ipv6 ospf neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
  This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)
  The default value is 1.
  Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub areas.
- Cost from the ASBR to an external network segment (that is, the metric of an external route)
  By default, the metric of a redistributed BGP route is 1, the metric of other types of redistributed routes is 20, and the route type is Type 2 External.
  Run the **default-metric** command to modify the default metric of the external route.
  Use the **metric**,**metric-type**, and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.
- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
  By default, the metric is 1, and the route type is Type 2 External.
  Use the **metric**,**metric-type**, and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.

- Use the **metric** and **metric-type** parameters of **default-information originate** in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.
  Use the **metric** and **metric-type** parameters of **default-information originate** in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.

OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

7.3.3 Enhanced Security and Reliability

Use functions such as authentication and BFD correlation to enhance security, stability, and reliability of OSPF.

Working Principle

Authentication

OSPFv3 uses the authentication mechanism, that is, IP authentication header (AH) and IP Encapsulating Security Payload (ESP), provided by IPv6 to prevent unauthorized routers that access the network and hosts that forge OSPF packets to participate in OSPF routing. OSPF packets received on the OSPF interface (or at both ends of a virtual link) are authenticated. If authentication fails, the packets are discarded and the adjacency cannot be set up.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

MTU Verification

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

Two-Way Maintenance

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

Concurrent neighbor Interaction Restriction

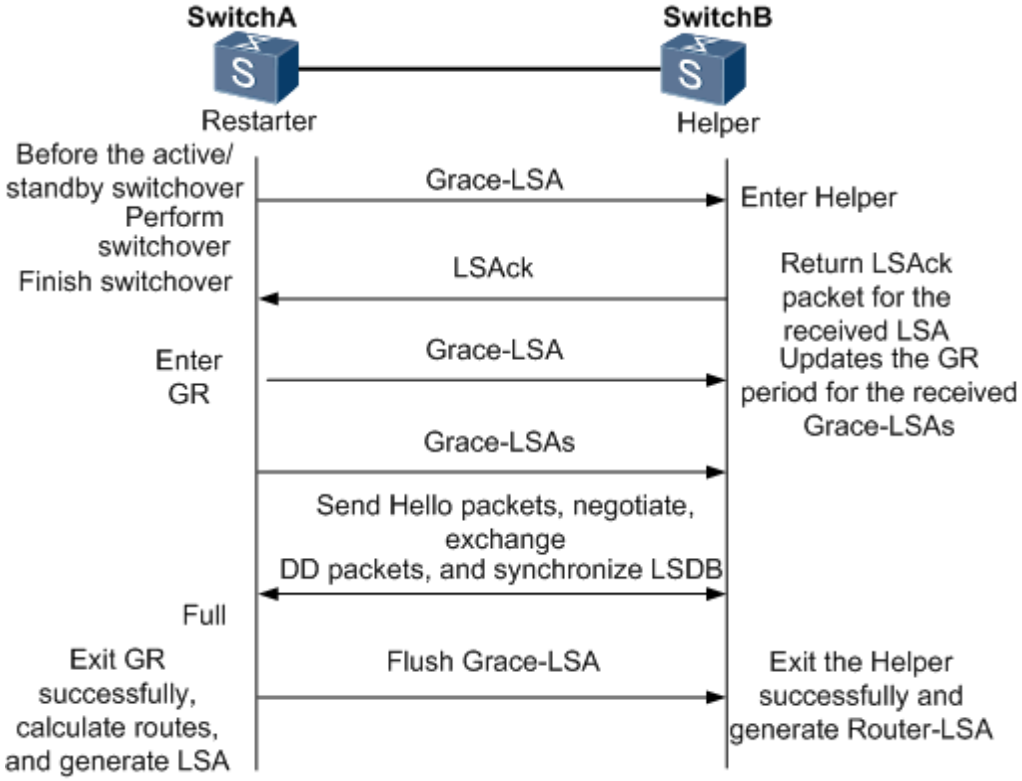
When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 7-6Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a Grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the Full state, the router can exit the GR process successfully.

Fast Hello

After a link fault occurs, it takes a period of time (about 40s) before OSPF can sense the death of the neighbor. Then, OSPF advertises the information and re-computes the SPT. During this period, traffic is interrupted.

- After the fast Hello function is enabled (that is, the neighbor dead interval is set to 1s), OSPF can sense the death of a neighbor within 1s once a link is faulty. This greatly accelerates route convergence and prevents traffic interruption.

Related Configuration

OSPF Packet Authentication

By default, authentication is disabled.

- Run the **area authentication** command to enable authentication in the entire area so that the authentication function takes effect on all interfaces in this area. If authentication is enabled in area 0, the function also takes effect on the virtual link.
- Run the **area encryption** command to enable encryption and authentication in the entire area so that the encryption**and** authentication functions take effect on all interfaces in this area. If encryptionand authentication are enabled in area 0, the functions also take effect on the virtual link.
- Run the **ipv6 ospf authentication** command to enable authentication on an interface. This configuration takes precedence over the area-based configuration.
- Run the **ipv6 ospf encryption** command to enable encryptionand authentication on an interface. This configuration takes precedence over the area-based configuration.
- Use the **authentication** parameter in the **area virtual-link** command to enable authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.
- Use the **encryption** parameter in the **area virtual-link** command to enable encryptionand authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.

MTU Verification

By default, MTU verification is disabled.

Run the **ipv6 ospf mtu-ignore** command to disable MTU verification on an interface.

Two-Way Maintenance

By default, bidirectional maintenance is enabled.

Run the **two-way-maintain** command to enable two-way maintenance.

Concurrent neighbor Interaction Restriction

Run the **max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with the current OSPF process. The default value is 5.

Run the **ipv6 router ospf max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with all OSPF processes on the router. The default value is 10.

GR

By default, the restarter function is disabled, and the helper function is enabled.

Run the **graceful-restart** command to configure the restarter function.

Run the **graceful-restart helper** command to configure the helper function.

Fast Hello

By default, the neighbor dead interval on the interface is 40s.

Run the **ipv6 ospf dead-interval minimal hello-multiplier** command to enable the Fast Hello function on an interface, that is, the neighbor dead interval is 1s.

7.3.4 Network Management Functions

Use functions such as the MIB and Syslog to facilitate OSPF management.

Working Principle

MIB

MIB is the device status information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound with only one OSPF process.

Trap

A trap message is a notification generated when the system detects a fault. This message contains the related fault information.

If the trap function is enabled, the router can proactively send the trap messages to the network management device.

Syslog

The Syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process that the OSPF adjacency is set up and maintained.

Related Configuration

MIB

By default, the MIB is bound with the OSPF process with the smallest process ID.

Run the **enable mib-binding** command to bind the MIB with the current OSPF process.

Trap

By default, all traps functions are disabled, and the device is not allowed to send OSPF traps.

Run the **snmp-server enable traps ospf** command to allow the device to send OSPF traps.

Run the **enable traps** command to enable a specified trap function for an OSPF process.

Syslog

By default, the Syslog is allowed to record the adjacency changes.

Run the **log-adj-changes** command to allow the Syslog to record the adjacency changes.

7.4 Configuration

Configuration	Description and Command	
Configuring OSPF Basic Functions	(Mandatory)It is used to build an OSPF routing domain.	
	ipv6routerospf	Creates an OSPF process.
	router-id	Configures a router ID.
	ipv6 ospfarea	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	(Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ipv6 ospf network	Defines the network type.
	ipv6 ospf neighbor	Specifies a neighbor.
	ipv6 ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	(Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring the Stub Area and NSSA Area	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	areastub	Configures a stub area.
Configuring Route Summarization	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	arearange	Summarizes routes that are advertised between areas.
	summary-prefix	Summarizes routes that are introduced through redistribution.
Configuring Route Filtering	(Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-list in	Filters received LSAs.
Modifying the Route Cost and AD	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-cost reference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ipv6 ospf cost	Modifies the cost in the outbound direction of an interface.

Configuration	Description and Command	
	areadefault-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	distance	Modifies the OSPF AD.
Enabling Authentication	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	area authentication	Enables authentication and sets the authentication mode in an area.
	area encryption	Enables encryption and authentication and sets the authentication mode in an area.
	ipv6 ospf authentication	Enables authentication and sets the authentication mode on an interface.
	ipv6 ospf encryption	Enables encryption and authentication and sets the authentication mode on an interface.
Modifying the Maximum Number of Concurrent Neighbors	(Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	
	max-concurrent-dd	Modifies the maximum number of con current neighbors on the current OSPF process.
	ipv6 router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.
Disabling MTU Verification	(Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ipv6 ospf mtu-ignore	Disables MTU verification on an interface.
Enabling Two-Way Maintenance	(Optional) It is used to prevent termination of the adjacency due to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling GR	(Optional) It is used to retain OSPF routing forwarding during restart or active/standby switchover of the OSPF processes to prevent traffic interruption.	
	graceful-restart	Enables the restarter function.
	graceful-restart helper	Enables the helper function.
Enabling Fast Hello	(Optional) It is used to quickly discover the death of a neighbor to prevent traffic interruption when a link is faulty.	
	ipv6 ospf dead-intervalminimal hello-multiplier	Enabling the Fast Hello function on an interface.
Configuring Network	(Optional) The configurations enable users to use the SNMP network management	

Configuration	Description and Command	
Management Functions	software to manage OSPF.	
	enable mib-binding	Bind MIB to the OSPF process.
	enable traps	Enables the trap function of the OSPF process.
	log-adj-changes	Allows the syslogs to record the changes in adjacency status.
Modifying Protocol Control Parameters	(Optional) You are advised not to modify protocol control parameters unless necessary.	
	ipv6 ospf hello-interval	Modifies the Hello interval on an interface.
	ipv6 ospf dead-interval	Modifies the neighbor death interval on an interface.
	ipv6 ospf transmit-delay	Modifies the LSU packet transmission delay on an interface.
	ipv6 ospf retransmit-interval	Modifies the LSU packet retransmission interval on an interface.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the inter-area route computation delay.

7.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv6 unicast routing service for users on the network.

Notes

- Ensure that the IPv6 routing function is enabled, that is, **ipv6 routing** is not disabled; otherwise, OSPF cannot be enabled.
- IPv6 must be enabled on the interface.
- It is strongly recommended that you manually configure the router ID.

Configuration Steps

Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.
- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Enabling OSPF on an Interface and Specifying an Area ID

- Mandatory.
- The configuration is mandatory for every router.

Verification

- Run the **show ipv6 route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv6 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**ipv6 router ospf***process-id*
Parameter Description	*process-id:* Indicates the OSPFv3 process ID. If the process ID is not specified, process 1 is enabled.
Command Mode	Global configuration mode
Usage Guide	After enabling the OSPFv3 process, the device enters the routing process configuration mode.

Configuring a Router ID

Command	**router-id***router-id*
Parameter Description	*router-id:* Indicates the ID of the device, which is expressed in the IPv4 address.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every device where OSPFv3 run must be identified by using a router ID. You can configure any IPv4 address as the router ID of the device, and ensure that the router ID is unique in an AS. If multiple OSPFv3 processes run on the same device, the router ID of each process must also be unique. After the router ID changes, OSPF performs a lot of internal processing. Therefore, you are advised

	not to change the router ID unless necessary. When an attempt is made to modify the router ID, a prompt is displayed, requesting you to confirm the modification. After the OSPFv3 process is enabled, you are advised to specify the router ID before configuring other parameters of the process.

Enabling OSPF on an Interface and Specifying an Area ID

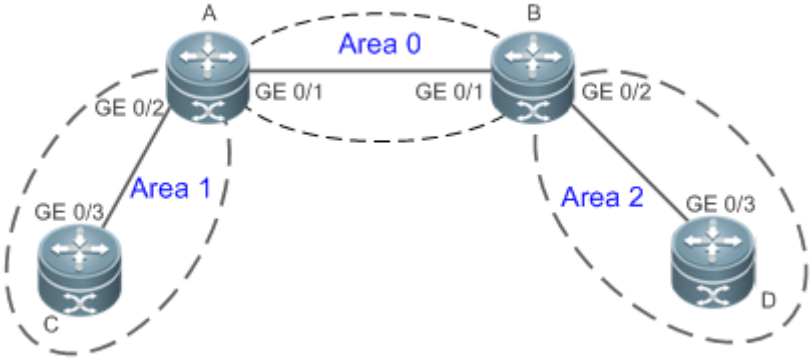
Command	**ipv6 ospf***process-id* **area***area-id* [**instance***instance-id*]
Parameter Description	*process-id*: Indicates the ID of an OSPFv3 process. The value ranges from 1 to 65,535. **Area***area-id:* Indicates the ID of the OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix. **Instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	Run this command in interface configuration mode to enable the interface to participate in OSPFv3, and then run the **ipv6 router ospf** command to configure the OSPFv3 process. After the OSPFv3 process is configured, the interface will automatically participate in the related process. Run the **no ipv6 ospfarea** command so that the specified interface no longer participates in the OSPFv3 routing process. Run the **no ipv6 router ospf** command so that all interfaces no longer participate in the OSPFv3 routing process. The adjacency can be set up only between devices with the same *instance-id*. After this command is configured, all prefix information on the interface will participate in the OSPFv3 process.

Creating a Virtual Link

Command	**area** *area-id***virtual-link***router-id* [**hello-interval** *seconds*] [**dead-interval***seconds*] [**retransmit-interval***seconds*] [**transmit-delay***seconds*] [**instance***instance-id*] [**authenticationipsec spi***spi*[**md5|sha1**] [**0|7**] *key*] [**encryption ipsec spi***spi* **esp** [**null**|[**des | 3des**] [**0** | **7**]*des-key*][**md5|sha1**] [**0|7**] *key*]
Parameter Description	*area-id:* Indicates the ID of the area where the virtual link is located. It can be an integer or an IPv4 prefix. *router-id:* Indicates the router ID of the neighbor connected to the virtual link. **dead-interval***seconds:* Indicates the time that the local interface of the virtual link detects the failure of the neighbor. The unit is second. The value ranges from 1 to 65,535. **hello-interval** *seconds:* Indicates the time that the Hello packet is sent on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **retransmit-interval** *seconds:* Indicates the interval at which the LSA is retransmitted on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **transmit-delay** *seconds:* Indicates the delay after which the LSA is sent on the local interface of the virtual link. The unit is second. The value ranges from 1 to 65,535. **instance***instance-id:* Indicates the ID of the instance corresponding to the virtual link. The value

	ranges from 0 to 255. A virtual link cannot be set up between devices with different instance IDs. *spi:* Indicates the security parameter index (SPI). The value ranges from 256 to 4,294,967,295. md5: Enables message digit 5 (MD5) authentication. sha1: Enables Secure Hash Algorithm 1 (SHA1) authentication. 0: Indicates that the key is displayed in plain text. 7: Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key. **null:** Indicates that no encryption mode is used. **des:** Specifies the DES encryption mode. **3des:** Specifies the 3DES encryption mode. *des-key:* Indicates the encryption key.
Command Mode	OSPF routing process configuration mode
Usage Guide	In an OSPFv3 AS, all areas must be connected to the backbone area to properly learn the routing information of the entire OSPFv3 AS. If an area cannot be directly connected to the backbone area, the virtual link can be used to connect this area to the backbone area. The area where the virtual link is located cannot be a stub or NSSA area. At both ends of neighbors between which the virtual link is set up, settings of **hello-interval, dead-interval**, and **instance** must be consistent; otherwise, the adjacency cannot be set up properly.

Configuration Example

Scenario	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 2001:1::1/64 GE 0/2 2001:2::1/64 B: GE 0/1 2001:1::2/64 GE 0/2 2001:3::1/64 C: GE 0/3 2001:2::2/64 D: GE 0/3 2001:3::2/64
Configuration Steps	● Configure the interface IP addresses on all routers. ● Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.) ● Configure the OSPF instances and router IDs on all routers. ● Enable OSPF on the interfaces configured on all routers.

A	A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#ipv6 enable A(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::1/64 A(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ipv6 enable A(config-if-GigabitEthernet 0/2)#ipv6 address 2001:2::1/64 A(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 1 A(config-if-GigabitEthernet 0/2)#exit A(config)#ipv6 router ospf 1 A(config-router)#router-id1.1.1.1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ipv6 enable B(config-if-GigabitEthernet 0/1)#ipv6 address 2001:1::2/64 B(config-if-GigabitEthernet 0/1)#ipv6 ospf 1 area 0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ipv6 enable B(config-if-GigabitEthernet 0/2)#ipv6 address 2001:3::1/64 B(config-if-GigabitEthernet 0/2)#ipv6 ospf 1 area 2 B(config-if-GigabitEthernet 0/2)#exit B(config)#ipv6 router ospf 1 B(config-router)#router-id2.2.2.2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ipv6 enable C(config-if-GigabitEthernet 0/3)#ipv6 address 2001:2::2/64 C(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 1

	C(config-if-GigabitEthernet 0/3)#exit C(config)#ipv6 router ospf 1 C(config-router)#router-id3.3.3.3
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ipv6 enable D(config-if-GigabitEthernet 0/3)#ipv6 address 2001:4::2/64 D(config-if-GigabitEthernet 0/3)#ipv6 ospf 1 area 2 D(config-if-GigabitEthernet 0/3)#exit D(config)#ipv6 router ospf 1 D(config-router)#router-id4.4.4.4
Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● Verify that 2001:2::2/64 can be pinged successfully on Router D.
A	A#show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/BDR 00:00:30 0 GigabitEthernet 0/1 3.3.3.31 Full/BDR 00:00:35 0 GigabitEthernet 0/2 A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:3::/64 [110/20] via FE80::2D0:F8FF:FE22:4524, GigabitEthernet 0/1

B

```
B# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State           Dead Time   Instance ID   Interface
1.1.1.11   Full/DR        00:00:30    0           GigabitEthernet 0/1
4.4.4.41   Full/BDR       00:00:35    0           GigabitEthernet 0/2

B#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

O  IA2001:2::/64 [110/20] via FE80::2D0:F8FF:FE22:4536, GigabitEthernet 0/1
```

C

```
C# show ipv6 ospf neighbor
OSPFv3 Process (1), 1 Neighbors, 1 is Full:
Neighbor ID    Pri   State           Dead Time   Instance ID   Interface
1.1.1.11   Full/DR        00:00:30    0           GigabitEthernet 0/3

C#show ipv6 route ospf

IPv6 routing table name - Default - 0 entries
Codes:  C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area
```

	O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3 O IA2001:3::/64 [110/3] via FE80::2D0:F8FF:FE22:4537, GigabitEthernet 0/3
D	D# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:30 0 GigabitEthernet 0/3 D#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA2001:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 O IA2001:2::/64 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/3 D# D#ping 2001:2::2 Sending 5, 100-byte ICMP Echoes to 2001:2::2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 5/9/14 ms.

Common Errors

- IPv6 is disabled on the interface.
- OSPF cannot be enabled because the IPv6 unicast routing function is disabled.
- The area IDs enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.

7.4.2 Setting the Network Type

Configuration Effect

- If the physical network is X.25, Frame Relay, or ATM, OSPF can also run to provide the IPv6 unicast routing service.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends multicast OSPF packets, automatically discovers neighbors, and elects a DR and a BDR.
- The P2P network sends multicast OSPF packets and automatically discovers neighbors.
- The NBMA network sends unicast OSPF packets. Neighbors must be manually specified, and a DR and a BDR must be elected.
- The P2MP network (without carrying the **non-broadcast** parameter) sends multicast OSPF packets. Neighbors are automatically discovered.
- The P2MP network (carrying the **non-broadcast** parameter) sends unicast OSPF packets. Neighbors must be manually specified.

Configuration Steps

Configuring the Interface Network Type

- Optional.
- Perform this configuration on routers at both ends of the link.

Configuring a Neighbor

- (Optional)If the interface network type is set to NBMA or P2MP (carrying the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (carrying the **non-broadcast** parameter) network.

Configuring the Interface Priority

- (Optional)You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

Verification

- Run the **show ipv6 ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ipv6 ospf network** {**broadcast	non-broadcast** |**point-to-point	point-to-multipoint**[**non-broadcast**]}[**instance***instance-id*]
Parameter Description	**broadcast**: Indicates the broadcast network type. **non-broadcast:** Indicates the non-broadcast network type. **point-to-multipoint**: Indicates the point-to-multipoint (P2MP) network type. **point-to-multipoint non-broadcast:** Indicates the P2MP non-broadcast network type. **point-to-point:** Indicates the point-to-point (P2P) network type. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	You can configure the network type of an interface based on the actual link type and topology.

Configuring a Neighbor

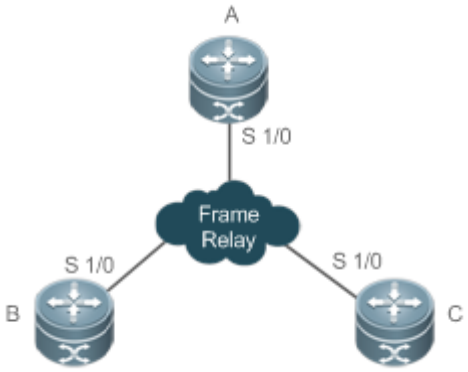
Command	**ipv6 ospf neighbor** *ipv6-address*{ [**cost***cost*]	[**poll-interval***seconds*	**priority***value*] }[**instance***instance-id*]
Parameter Description	*ip-address*: Indicates the link address of theneighborinterface. **cost***cost***:** Indicates the cost required from the P2MP network to each neighbor. The cost is not defined by default. The cost configured on the interface is used. The value ranges from 1 to 65,535. Only a P2MP network supports this option. **poll-interval** *seconds*: Indicates the neighbor polling interval. The unit is second. The value ranges from 1 to 2,147,483,647. Only the non-broadcast (NBMA) network supports this option. **priority** *value***:** Indicates the priority value of the non-broadcast network neighbor. The value ranges from 0 to 255. Only the non-broadcast network (NBMA) supports this option. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	You can configure neighbor parameters based on the actual network type.

Configuring the Interface Priority

Command	**ipv6 ospf priority** *number-value*[**instance***instance-id*]
Parameter Description	*number-value*: Indicates the priority of the interface. The value ranges from 0 to 255. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	On a broadcast network, a DR or BDR must be elected. During the DR/BDR election, the device with a higher priority will be preferentially elected as a DR or BDR. If the priority is the same, the device with a larger router ID will be preferentially elected as a DR or BDR. A device with the priority 0 does not participate in the DR/BDR election.

Configuration Example

Configuring the Interface Network Type

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Set the interface network type to P2MP on all routers.
A	`A#configure terminal` `A(config)# interface Serial1/0` `A(config-Serial1/0)# encapsulation frame-relay` `A(config-Serial1/0)# ipv6 ospf network point-to-multipoint`
B	`B#configure terminal` `B(config)# interface Serial1/0` `B(config-Serial1/0)# encapsulation frame-relay` `B(config-Serial1/0)# ipv6 ospf network point-to-multipoint`
C	`C#configure terminal` `C(config)# interface Serial1/0` `C(config-Serial1/0)# encapsulation frame-relay` `C(config-Serial1/0)# ipv6 ospf network point-to-multipoint`
Verification	● Verify that the interface network type is P2MP.

A	A#show ipv6 ospf interface Serial1/0 Serial1/0 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0 Router ID 192.168.22.30,Network Type POINTOMULTIPOINT, Cost: 1 Transmit Delay is 1 sec, State Point-To-Point, Priority 1 Timer interval configured, Hello 30, Dead 120, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (non-broadcast), but neighbors are not specified.

7.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- Introduce unicast routes for other AS domains to the OSPF domain to provide the unicast routing service to other AS domains for users in the OSPF domain.
- In the OSPF domain, inject a default route to another AS domain so that the unicast routing service to another AS domain can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Configuring External Route Redistribution

- (Optional)This configuration is mandatory if external routes of the OSPF domain should be introduced to the ASBR.
- Perform this configuration on an ASBR.

Generating a Default Route

- (Optional)Perform this configuration if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.
- Perform this configuration on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ipv6 route ospf** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ipv6 route ospf** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv6 unicast service to other AS domains is correct.

Related Commands

Configuring Route Redistribution

Command	**redistribute** { **connected** | **ospf***process-id*| **rip** | **static**}[**match** {**internal | external** [**1|2**]**} | metric** *metric-value***|metric-type** {**1**|**2**} | **route-map** *route-map-name* |**tag***tag-value*]
Parameter Description	**connected:** Indicates redistribution from direct routes. **ospf***process-id:* Indicates redistribution from OSPF.**process-id** specifies an OSPF instance. The value ranges from 1 to 65535. 1-65535 **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes. **match:** Used only when OSPF routes are redistributed. Only the routes that match the specified criteria are redistributed. By default, all OSPF routes can be redistributed. **metric***metric-value:* Indicates the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type** {**1**|**2**}: Indicates the external route type, which can be E-1 or E-2. **route-map***route-map-name:* Sets the redistribution filtering rules. **tag***tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4294967295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the device supports multiple routing protocols, collaboration between protocols is very important. To run multiple routing protocols concurrently, the device must be able to redistribute routing information of a protocol to another protocol. This applies to all routing protocols. During redistribution of IS-IS routes, **level-1**,**level-2**, or **level-1-2** can be configured to indicate that IS-IS routes of the specified level(s) will be redistributed. By default, IS-IS routes of level 2 are redistributed. During redistribution of OSPFv3 routes, **match** can be configured to indicate that OSPFv3 routes of the specified sub-type will be redistributed. By default, all types of OSPFv3 routes are redistributed. For the **level** parameter configured during redistribution of IS-IS routes and the match parameter configured

	during redistribution of OSPFv3 routes, the routes are matched against the route map only when the sub-type of the routes are correct. During configuration of route redistribution, the **match**rules configured in route map configuration mode areused based on the original information of routes. The priorities of **tag**, **metric** and **metric-type** in the route redistribution configuration are lower than the priority of the**set** rulesconfigured in route map configuration mode. The **set metric** value of the associated routemap should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted. For example, if **redistribute isis 112 level-2** is configured, the **no redistribute isis 112 level-2** command only restores the default value of **level-2**. As level-2 itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding no form of the command is executed. To delete the entire command, you need to run the **no redistribute isis 112** command.

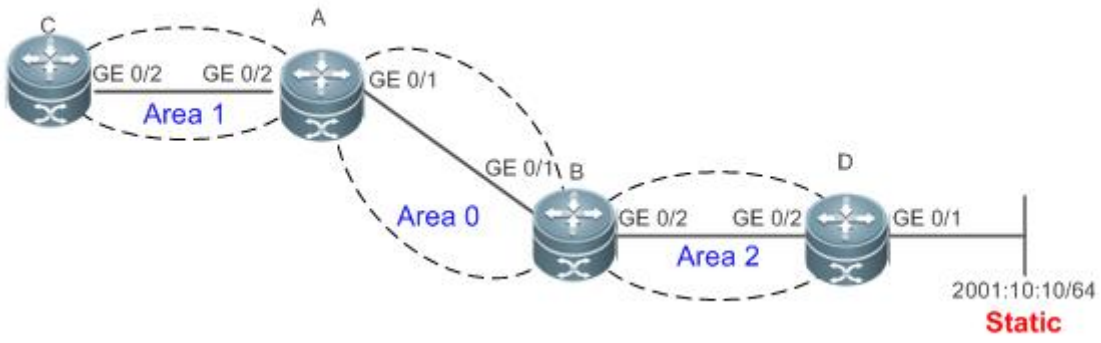
Introducing a Default Route

Command	**default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map***map*]
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. By default, the metric of the default route is 1. **metric-type***type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the **redistribute** or **default-information** command is executed, the OSPFv3-enabled router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To have the ASBR generate a default route, configure the **default-information originate** command. If **always** is specified, the OSPFv3 process advertises an external default route to neighbors no matter whether a default route exists in the core routing table. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ipv6 ospf database** command to display the OSPFv3 link status database. On an OSPFv3 neighbor, you can run the **show ipv6 route ospf** command to see the default route. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command.

	OSPFv3 has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination network have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ipv6 route ospf** command displays only the Type 1 route. A router in a stub area cannot generate an external default route.

Configuration Example

↘ Configuring Route Redistribution

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Introduce an external static route to Router D.
D	`D#configure terminal` `D(config)#ipv6 router ospf 1` `D(config-router)# redistribute static`
Verification	● On Router D, run the **show ipv6ospf database external brief** command to verify that an LSA corresponding to an external route is generated. ● On Router C, run the **show ipv6 route ospf** command to verify that the external static route has been introduced.

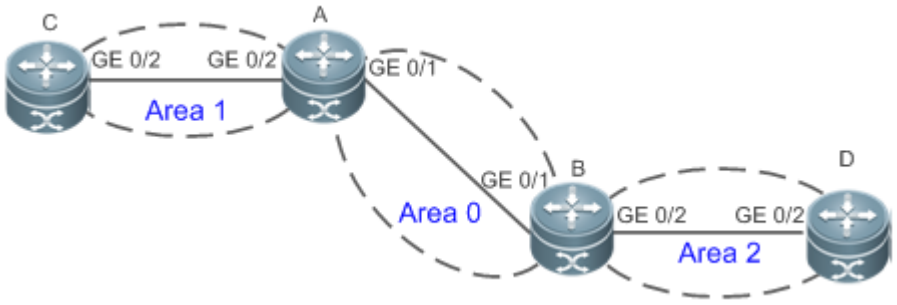
D

```
D#show ipv6 ospf database external

          OSPFv3 Router with ID (4.4.4.4) (Process 1)

              AS-external-LSA

  LS age: 7

  LS Type: AS-External-LSA

  Link State ID: 0.0.0.6

  Advertising Router: 4.4.4.4

  LS Seq Number: 0x80000001

  Checksum: 0x9C1F

  Length: 36

    Metric Type: 2 (Larger than any link state path)

    Metric: 20

    Prefix: 2001:10:10::/64

    Prefix Options: 0 (-|-|-|-)
```

C

```
C#show ipv6 route ospf


IPv6 routing table name - Default - 0 entries

Codes:  C - Connected, L - Local, S - Static

       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       IA - Inter area


O  E2  2001:10:10::/64 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2
```

Configuring the Default Route

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers. ● Configure the OSPF basic functions on all routers. ● Configure the default route on Router D.
D	`D#configure terminal` `D(config)#ipv6 router ospf 1` `D(config-router)#default-information originate always`
Verification	● On Router D, run the **show ipv6ospf database external brief** command to verify that an LSA corresponding to the default route is generated. ● On Router C, run the **show ipv6 route ospf** command to verify that the OSPF default route exists.
D	`D#show ipv6 ospf database external` `OSPFv3 Router with ID (4.4.4.4) (Process 1)` `AS-external-LSA` `LS age: 3` `LS Type: AS-External-LSA` `Link State ID: 0.0.0.7` `Advertising Router: 4.4.4.4` `LS Seq Number: 0x80000001` `Checksum: 0x1839` `Length: 32` `Metric Type: 2 (Larger than any link state path)` `Metric: 1` `Prefix: ::/0` `Prefix Options: 0 (-|-|-|-)` `External Route Tag: 1`

C	C#show ipv6route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2::/0 [110/20] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Common Errors

- A route loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

7.4.4 Configuring the Stub Area

Configuration Effect

- Configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub area.
- A router in the stub area cannot introduce external routes.

Configuration Steps

↘ **Configuring a Stub Area**

- (Optional)Perform this configuration if you wish to reduce the size of the routing table on routers in the area.
- Perform this configuration on all routers in the same area.

Verification

↘ **Verifying the Stub Area**

- On a router in the stub area, run the **show ipv6 route** command to verify that the router is not loaded with any external routes.

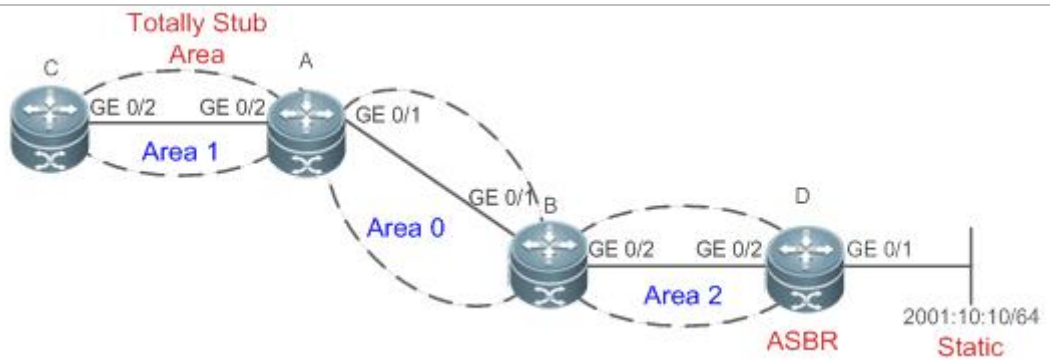
Related Commands

Configuring a Stub Area

Command	**area***area-id***stub** [**no-summary**]
Parameter Description	*area-id:* Indicates the ID of the stub area. The value can be an integer or an IPv4 prefix. **no-summary:** This option is valid only ona the ABR in a stub area. If this option is specified, the ABR only advertises one Type 3 LSA indicating the default route to the stub area, and does not advertise other Type 3 LSAs.
Command Mode	OSPF routing process configuration mode
Usage Guide	An area located on the stub of a network can be configured as a stub area. You must run the **area stub** command on all routers in a stub area. Devices in a stub area cannot learn the external routes (Type 5 LSAs) of the AS. In practice, external routes take up a large proportion of the link status database. Therefore, devices in a stub area can learn only a small amount of routing information, which reduces the amount of system resources required to run the OSPFv3 protocol. By default, an ABR in a stub area will generate a Type 3 LSA indicating the default fault, and advertise the LSA to the stub area. In this way, devices in the stub area can access devices outside the AS. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR.

Configuration Example

Configuring a Stub Area

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.

D	D#configure terminal D(config)#ipv6 router ospf 1 D(config-router)#redistribute static
A	A# configure terminal A(config)#ipv6 router ospf 1 A(config-router)#area 1 stubno-summary
C	C#configure terminal C(config)#ipv6 router ospf 1 C(config-router)#area 1 stub
Verification	● On Router C, run the **show ipv6 route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Router D.
C	C#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O IA::/0 [110/3] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/2

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

7.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- The address range of the summarize route may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table or shield or filter routes.

Configuration Steps

Configuring Inter-Area Route Summarization

- (Optional) Perform this configuration when routes of the OSPF area need to be summarized.
- Unless otherwise required, perform this configuration on an ABR in the area where routes to be summarized are located.

Configuring External Route Summarization

- (Optional) Perform this configuration when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, perform this configuration on an ASBR, to which routes that need to be summarized are introduced.

Verification

- Run the **show ipv6 route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

Configuring Inter-Area Route Summarization

Command	**area***area-id* **range***ipv6-prefix*/*prefix-length* [**advertise**|**not-advertise**]
Parameter Description	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The value can be an integer or an IPv4 prefix. *ipv6-prefix*/*prefix-length*: Indicates the range of IP addresses to be summarized. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR, and is used to summarize multiple routes in an area into a route and advertise this route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route. You can configure route summarization commands for multiple areas. This simplifies routes in the entire

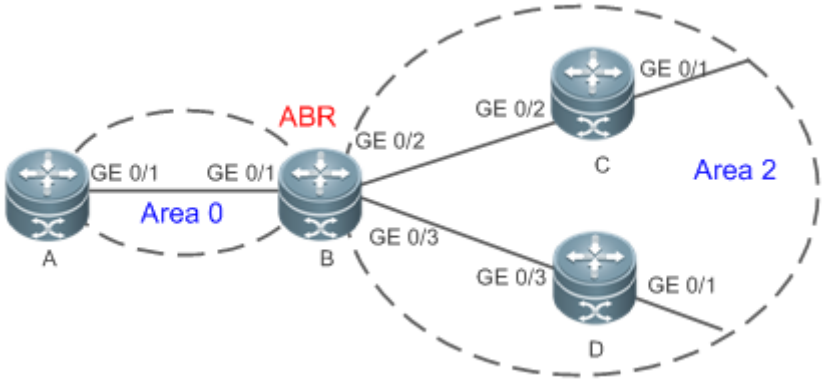
	OSPF routing domain, and improves the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

Command	**summary-prefix***ipv6-prefix/prefix-length* [**not-advertise** | **tag** *number*]
Parameter Description	*ipv6-prefix/prefix-length*: Indicates the range of IP addresses to be summarized. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised. **tag***number:* Specifies the tag value of the route that is redistributed into the OSPFv3 routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPFv3 routing process, each route is advertised to the OSPFv3 routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertise only one summarized route to significantly reduce the size of the routing table. **area range** summarizes the routes between OSPFv3 areas, whereas **summary-prefix** summarizes external routes of the OSPFv3 routing domain. When configured on the NSSA ABR translator, **summary-prefix** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-prefix** summarizes only redistributed routes.

Configuration Example

Configuration Steps



Remarks	The interface IPv6 addresses are as follows: B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64 C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64 D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Summarize routes of area 2 on Router B.
B	`B#configure terminal` `B(config)#ipv6 router ospf 1` `B(config-router)#area 2 range 2001:16::/64`
Verification	On Router A, check the routing table and verify that the entry 2001:16::/64 is generated and other routes do not exist.
A	`A#show ipv6 route ospf` `IPv6 routing table name - Default - 0 entries` `Codes:  C - Connected, L - Local, S - Static` `R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route` `N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2` `E1 - OSPF external type 1, E2 - OSPF external type 2` `SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2` `IA - Inter area` `O  IA  2001:16::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1`

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

7.4.6 Configuring Route Filtering

Configuration Effect

- Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are

generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Steps

Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users need to be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, perform this configuration on an ABR in the area where filtered routes are located.

Configuring Redistributed Route Filtering

- (Optional) Perform this configuration if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, perform this configurationon an ASBR to which filtered routes are introduced.

Configuring Learned Route Filtering

- (Optional) Perform this configuration if users need to be restricted from accessing a specified destination network.
- Unless otherwise required, perform this configurationon a router that requires route filtering.

Verification

- Run the **show ipv6 route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

Configuring a Passive Interface

Command	**passive-interface** {**default** | *interface-typeinterface-number* }
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interfaces will be configured as passive interfaces.
Command Mode	OSPF routing process configuration mode
Usage Guide	When an interface is configured as a passive interface, it no longer sends or receives Hello packets. This command takes effect only on an OSPFv3-enabled interface, and not on a virtual link.

Configuring Redistributed Route Filtering

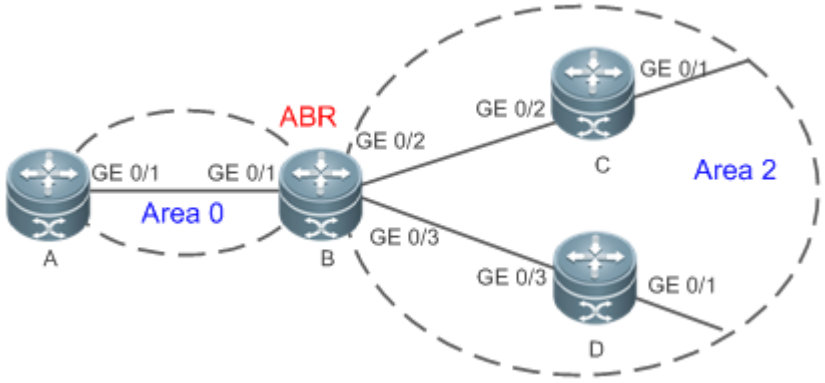
Command	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**out**[**bgp** | **connected** |**isis**[*area-tag*]| **ospf** *process-id*| **rip** | **static**]
Parameter Description	*name*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefix list for filtering. **bgp | connected | isis**[*area-tag*] | **ospf** process-id| **rip** | **static**: Indicates the source of routes to be filtered.
Command	OSPF routing process configuration mode

Mode	
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPFv3. The **distribute-list out** command itself does not redistribute routes, and is generally used together with the **redistribute** command. The ACL and the prefix list filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefix list cannot be configured to filter the same routes.

Configuring Learned Route Filtering

Command	**distribute-list**{*name* | **prefix-list** *prefix-list-name*}**in** [*interface-typeinterface-number*]
Parameter Description	*name*: Uses the ACL for filtering. **prefix***prefix-list-name*: Uses the prefix list for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL and the prefix list filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes on a specified interface, the prefix list cannot be configured to filter routes on the same interface. Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Example

Scenario	

Remarks	The interface IPv6 addresses are as follows: B: GE0/2 2001:16:2::1/64 GE0/3 2001:16:3::1/64 C: GE0/2 2001:16:2::2/64 GE0/1 2001:16:4::2/64 D: GE0/3 2001:16:3::2/64 GE0/1 2001:16:5::1/64

Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure route filtering.
A	`A#configure terminal` `A(config)#ipv6 access-list test` `A (config-ipv6-acl)#permit ipv6 2001:16:5::/64 any` `A(config)#ipv6 router ospf 1` `A(config-router)#distribute-list test in GigabitEthernet0/1`
Verification	● On Router A, check the routing table. Verify that only the entry 2001:16:5::/64 is loaded.
A	`A#show ipv6 route ospf` `IPv6 routing table name - Default - 0 entries` `Codes:  C - Connected, L - Local, S - Static` `R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route` `N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2` `E1 - OSPF external type 1, E2 - OSPF external type 2` `SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2` `IA - Inter area` `O  IA  2001:16:5::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1`

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated.

7.4.7 Modifying the Route Cost and AD

Configuration Effect

- Change the OSPF routes so that the traffic passes through specified nodes or bypasses specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- The OSPF basic functions must be configured.

- If you run the **ipv6 ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Steps

Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

Configuring the Default Metric for Redistribution

- Optional.
- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- Perform this configuration if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ipv6 ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ipv6 route** command to verify that the costs of external routes introduced by the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-cost reference-bandwidth** *ref-bw*
Parameter	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.

Description	
Command Mode	OSPF routing process configuration mode
Usage Guide	You can run the **ipv6 ospf cost** command in interface configuration mode to specify the cost of the interface. The priority of this cost is higher than that of the metric computed based on the reference bandwidth.

Configuring the Cost of an Interface

Command	**ipv6 ospf cost** *cost*[**instance***instance-id*]
Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535. **instance***instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	By default, the cost of an OSPFv3 interface is equal to 100 Mbps/Bandwidth, where Bandwidth is the bandwidth of the interface and configured by the **bandwidth** command in interface configuration mode. The costs of OSPF interfaces on several typical lines are as follows: ● 64 Kbps serial line: The cost is 1562. ● E1 line: The cost is 48. ● 10M Ethernet: The cost is 10. ● 100M Ethernet: The cost is 1. If you run the **ipv6 ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area***area-id* **default-cost***cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area.

Configuring the Default Metric for Redistribution

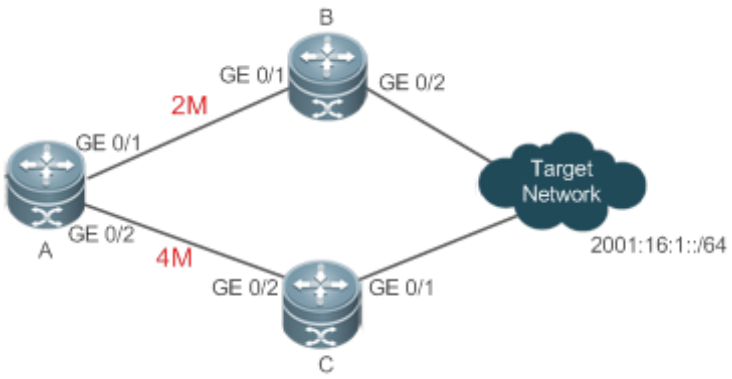
Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric** command must be used together with the **redistribute** command to modify the initial metrics of all redistributed routes. The **default-metric** command does not take effect on external routes that

	are injected to the OSPF routing domain by the **default-information originate** command. The default metric of a redistributed direct route is always 20.

Configuring the AD

Command	**distance** { *distance* | **ospf**{ [**intra-area***distance*] [**inter-area***distance*] [**external** *distance*]} }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area***distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	Use this command to specify different ADs for different types of OSPF routes. The AD allows different routing protocols to compare route priorities. A smaller AD indicates a higher route priority. The priorities of routes generated by different OSPFv3 processes must be compared based on ADs. If the AD of a route entry is set to 255, the route entry is not trustworthy and does not participate in packet forwarding.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.
A	`A#configure terminal` `A(config)#interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)#ipv6 ospf cost 10` `A(config)#interface GigabitEthernet 0/2` `A(config-if-GigabitEthernet 0/2)#ipv6 ospf cost 20`
Verification	● On Router A, check the routing table. The next hop of the optimum path to 2001:16:1::/64 is Router B.

A	A#show ipv6 route ospf IPv6 routing table name - Default - 0 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area O E2 2001:16:1::/64 [110/2] via FE80::2D0:F8FF:FE22:4547, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ipv6 ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

7.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

Configuration Steps

↘ Configuring Authentication

- Optional.
- Perform this configuration if a router accesses a network that requires authentication.

↘ Configuring Encryption

- Optional.
- Perform this configuration if a router accesses a network that requires encryption.

Configuring Virtual Link Authentication

- Optional.
- Perform this configuration if a router accesses a network that requires authentication.

Configuring Virtual Link Encryption

- Optional.
- Perform this configuration if a router accesses a network that requires encryption.

Verification

- If routers are configured with different authentication keys, run the **show ipv6 ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ipv6 ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring Area-based Authentication

Command	**area***area-id***authenticationipsec spi***spi*[**md5|sha1**] [**0	7**] *key*
Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **md5:** Enables MD5 authentication. **sha1:** Enables SHA1 authentication. **0:** Indicates that the key is displayed in plain text. **7:** Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports three authentication types: ● No authentication ● MD5 authentication ● SHA1 authentication Configuration of area-based authentication for OSPFv3 takes effect on all interfaces (except virtual links) in the area, but the interface-based authentication configuration takes precedence over the area-based configuration.

Configuring Area-based Encryption and Authentication

Command	**area***area-id***encryption ipsec spi***spi* **esp**[**null**|[**des**	**3des**][**0	7**] *des-key*][**md5|sha1**] [**0|7**] *key*
Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **null:** Indicates that no encryption mode is used.

	des: Indicates that the Data Encryption Standard (DES) mode is used. **3des:** Indicates that the Triple DES (3DES) mode is used. des-key: Indicates the encryption key. **md5**: Enables MD5 authentication. **sha1**: Enables SHA1 authentication. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. key: Indicates the authentication key.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports two encryption modes and two authentication modes. The two encryption modes are as follows: ● DES ● 3DES The two authentication modes are as follows: ● MD5 ● SHA1 Configuration of area-based encryption and authentication for OSPFv3 takes effect on all interfaces (except virtual links) in the area, but the interface-based encryption and authentication configuration takes precedence over the area-based configuration.

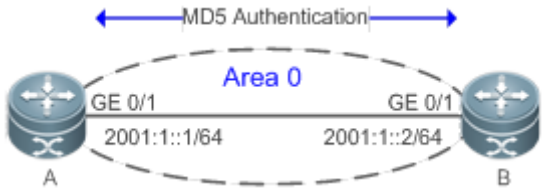
Configuring Interface-based Authentication

Command	**ipv6 ospfauthentication**[**null | ipsec spi***spi*[**md5|sha1**] [**0|7**]*key*][**instance***instance-id*]
Parameter Description	*area-id*: Indicates the area ID.The value can be an integer or an IPv4 prefix. *spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **md5:** Enables MD5 authentication. **sha1:** Enables SHA1 authentication. **0:** Indicates that the key is displayed in plain text. **7:** Indicates that the key is displayed in cipher text. *key:* Indicates the authentication key. **instance** *instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports three authentication types: ● No authentication ● MD5 authentication ● SHA1 authentication OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Configuring Interface-based Encryptionand Authentication

Command	**ipv6 ospfencryption ipsec spi***spi* **esp**[**null**|[**des**	**3des**][**0	7**] *des-key*][**md5|sha1**] [**0|7**] *key*[**instance***instance-id*]
Parameter Description	*spi*: Indicates the SPI. The value ranges from 256 to 4,294,967,295. **null:** Indicates that no encryption mode is used. **des:** Indicates that the DES mode is used. **3des:** Indicates that the3DES mode is used. des-key: Indicates the encryption key. **md5**: Enables MD5 authentication. **sha1**: Enables SHA1 authentication. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. key: Indicates the authentication key. **instance** *instance-id:* Indicates the ID of a specified OSPFv3 process of the interface. The value ranges from 0 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports two encryption modes and two authentication modes. The two encryption modes are as follows: ● DES ● 3DES The two authentication modes are as follows: ● MD5 ● SHA1 OSPFv3 encryption and authentication parameters configured on the local interface must be consistent with those configured on the interconnected interfaces.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure MD5 authentication for interfaces of all routers.
A	`A#configure terminal` `A(config)#interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)#ipv6 ospf authentication ipsec spi 256 md5 0123456789012345678901234567891 2`

B	B# configure terminal B(config)#interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)#ipv6 ospf authentication ipsec spi 256 md5 01234567890123456789012345678912
Verification	● On Router A and Router B, verify that the OSPF neighbor status is correct.
A	A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1
B	B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.1 1 Full/BDR 00:00:38 0 GigabitEthernet 0/1

Common Errors

- The configured authentication modes are inconsistent.
- The configured authentication keys are inconsistent.

7.4.9 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacency more quickly when a router is connected with a lot of other routers.
- Perform this configuration on a core router.

Verification

- Run the **show ipv6 ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

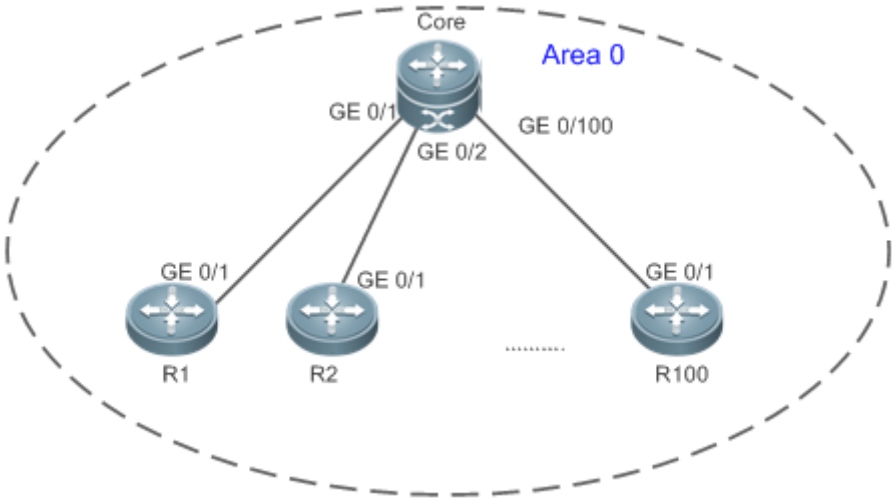
Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which each OSPF process can concurrently initiate or accept interaction.

Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**Ipv6 router ospf max-concurrent-dd***number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the Router Core, set the maximum number of concurrent neighbors to 4.

Core	`Core# configure terminal` `Core(config)# ipv6 router ospf max-concurrent-dd 4`
Verification	● On the Router Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

Common Errors

N/A

7.4.10 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- Perform this configuration on two routers with different interface MTUs.

Verification

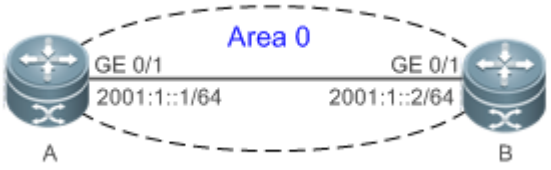
- The adjacency can be set up between routers with different MTUs.

Related Commands

↘ Disabling MTU Verification

Command	**Ipv6 ospf mtu-ignore**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure different MTUs for interfaces on two routers. ● Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400` `A(config-if-GigabitEthernet 0/1)#ipv6 ospf mtu-ignore`
B	`B# configure terminal` `B(config)# interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)# ipv6 mtu 1600` `B(config-if-GigabitEthernet 0/1)# ipv6 ospf mtu-ignore`
Verification	● On Router A, verify that the OSPF neighbor information is correct.
A	`A# show ipv6 ospf neighbor` `OSPFv3 Process (1), 1 Neighbors, 1 is Full:` `Neighbor ID Pri State Dead Time Instance ID Interface` `2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1`

Common Errors

N/A

7.4.11 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on all routers.

Verification

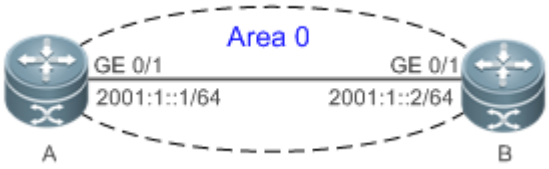
- Non-Hello packets can also be used to maintain the adjacency.

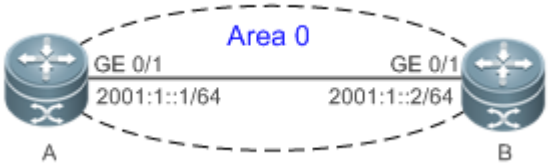
Related Commands

Enabling Two-Way Maintenance

Command	two-way-maintain
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed due to timeout.If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)
A	`A# configure terminal` `A(config)# ipv6 routerospf 1` `A(config-router)#two-way-maintain`
Verification	● When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
A	`A# show ipv6 ospfneighbor` `OSPFv3 Process (1), 1 Neighbors, 1 is Full:`

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)
A	`A# configure terminal` `A(config)# ipv6 routerospf 1` `A(config-router)#two-way-maintain`
Verification	● When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.
	`Neighbor ID Pri State Dead Time Instance ID Interface` `2.2.2.2 1 Full/DR 00:00:38 0 GigabitEthernet 0/1`

Common Errors

N/A

7.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active board to the standby board, traffic forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

↘ Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on routers where hot standby switchover is triggered or the OSPF process is restarted.

↘ Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- Perform this configuration on a router if hot standby switchover is triggered or the OSPF process is restarted on a neighbor of this router.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and the traffic is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and the traffic is not interrupted.

Related Commands

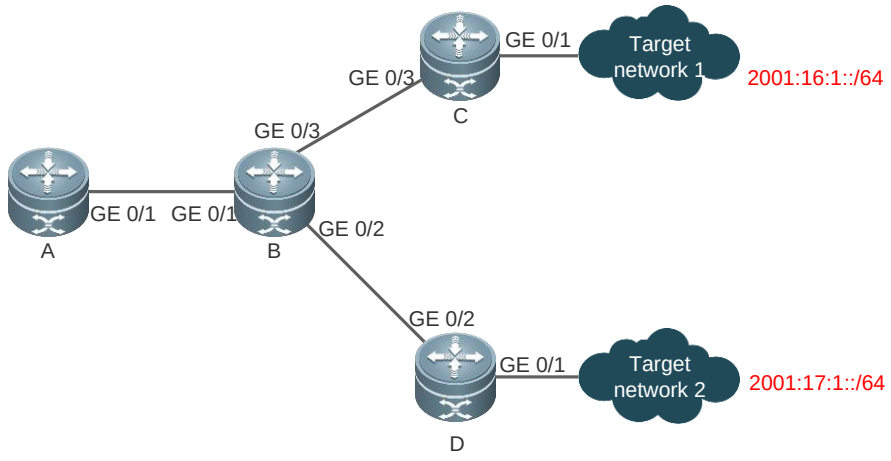
Configuring the OSPF GR Function

Command	**graceful-restart** [**grace-period***grace-period*|**inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the grace period varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence.After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations. Run the **graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. ● Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time. ● Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process. If the Fast Hello function is enabled, the GR function cannot be enabled.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable** |**strict-lsa-checking**	**internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR. After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Example

Scenario	

Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.) ● On Router B, enable the GR function.
B	`B# configure terminal` `B(config)# ipv6 router ospf1` `B(config-router)# graceful-restart`
Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

7.4.13 Configuring Network Management Functions

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP server before enabling the OSPF MIB function.
- You must enable the trap function of the SNMP server before enabling the OSPF trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

Configuration Steps

↘ Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- Perform this configuration on all routers.

↘ Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.
- Perform this configuration on all routers.

Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- Perform this configuration on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

Binding the MIB with the OSPF Process

Command	**enable mib-binding**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPFv2 MIB does not have the OSPFv3 process information. Therefore, you can perform operations only on a single OSPFv2 process through SNMP. By default, the OSPFv3 MIB is bound with the OSPFv3 process with the smallest process ID, and all user operations take effect on this process. If you wish to perform operations on a specified OSPFv3 process through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

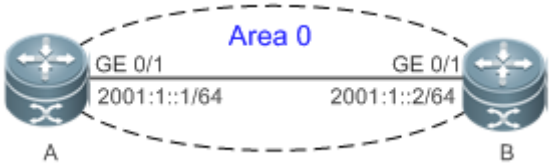
Command	**enable traps**[**error** [**IfConfigError| IfRxBadPacket	VirtIfConfigError	VirtIfRxBadPacket**]	**state-change**[**IfStateChange	NbrStateChange	NssaTranslatorStatusChange	VirtIfStateChange	VirtNbrStateChange	RestartStatusChange	NbrRestartHelperStatusChange	VirtNbrRestartHelperStatusChange**]]
Parameter Description	**IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **IfStateChange:** Indicates that interface state changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **NbrRestartHelperStatusChange:** Indicates that the state of the neighbor GR process changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes.

Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.
A	`A# configure terminal` `A(config)#snmp-server host 192.168.2.2 traps version 2c public` `A(config)#snmp-server community public rw` `A(config)#snmp-server enable traps` `A(config)#` `A(config)# ipv6 routerospf 10` `A(config-router)# enable mib-binding` `A(config-router)# enable traps`
Verification	● Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

N/A

7.4.14 Modifying Protocol Control Parameters

Configuration Effect

- Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

↘ **Configuring the Hello Interval**

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on routers at both end of a link.

↘ **Configuring the Dead Interval**

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- Perform this configuration on routers at both end of a link.

↘ **Configuring the LSU Retransmission Interval**

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

↘ **Configuring the LSA Generation Time**

- (Optional) You are advised to retain the default configuration.

↘ **Configuring the LSA Group Refresh Time**

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- Perform this configuration on an ASBR or ABR.

↘ **Configuring LSA Repeated Receiving Delay**

- (Optional) You are advised to retain the default configuration.

↘ **Configuring the SPF Computation Delay**

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

↘ **Configuring the Inter-Area Route Computation Delay**

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on all routers.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- Perform this configuration on all routers.

Verification

- Run the **show ipv6 ospf** and **show ipv6 ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ipv6ospf hello-interval***seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the Hello interval.

Configuring the Dead Interval

Command	**ipv6ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ipv6ospf transmit-delay***seconds*

Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmission delay and line propagation delay on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command. If the value of the Age field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring the LSU Retransmission Interval

Command	**ipv6ospf retransmit-interval***seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 0 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.
Command Mode	Interface configuration mode
Usage Guide	After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval**parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a high convergence requirement is raised when a link changes, you can set **delay-time** to a smaller value. You can also appropriately increase values of the preceding parameters to reduce the CPU usage. When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacinglsa-group** *seconds*
Parameter Description	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. In order to use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole. If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs processes upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 1000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 600,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs is large and the device load is heavy in an environment, properly configuring **transimit-time** and **transimit-count** can limit the number of LS-UPD packets flooded on a network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of **transimit-time** and increasing the value of **transimit-count** can accelerate the environment convergence.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival***arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the SPF Computation Delay

Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*

Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses. *spf-holdtime*: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: Indicates the metric of the summarized route.
Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-dela**y and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

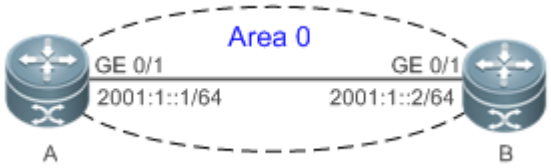
Configuring the Computation Delays of Inter-Area Routes and External Routes

Command	**timers throttle route**{**inter-area***ia-delay*|**ase***ase-delay*}
Parameter Description	**inter-area***ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000. **ase***ase-delay:* Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a strict requirement is raised for the network convergence time, use the default value. If a lot of inter-area or external routes exist on the network and the network is not stable, adjust the delays

	and optimize route computation to reduce the load on the device.

Configuration Example

Configuring the Hello Interval and Dead Interval

Scenario	
Configuration Steps	● Enable IPv6 on interfaces of all routers.(Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15` `A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50`
B	`B# configure terminal` `B(config)# interface GigabitEthernet 0/1` `B(config-if-GigabitEthernet 0/1)# ipv6 ospf hello-interval 15` `A(config-if-GigabitEthernet 0/1)# ipv6 ospf dead-interval 50`
Verification	● Check the interface parameters on Router A and Router B. Verify that the Hello interval is 10s and the dead interval is 50s. ● On Router A and Router B, verify that the OSPF neighbor information is correct.

A	A# show ipv6 ospf interface GigabitEthernet 0/1 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3346/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0 Router ID 1.1.1.1,Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1 Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1 A# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 2.2.2.21 Full/BDR 00:00:30 0 GigabitEthernet 0/1

B	B# show ipv6 ospf interface GigabitEthernet 0/1 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:f8ff:fe22:3446/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0 Router ID 2.2.2.2,Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State BDR, Priority 1 Timer interval configured, Hello 15, Dead 50, Wait 40, Retransmit 10 Hello due in 00:00:06 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 40 sent 40, DD received 17 sent 9 LS-Req received 1 sent 3, LS-Upd received 6 sent 5 LS-Ack received 3 sent 4, Discarded 1 B# show ipv6 ospf neighbor OSPFv3 Process (1), 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Instance ID Interface 1.1.1.11 Full/DR 00:00:38 0 GigabitEthernet 0/1

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

7.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears and resets an OSPF process.	**clear ipv6 ospf** [*process-id*]**process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ipv6 ospf** [*process-id*]

Description	Command
Displays information about the OSPF LSDB.	**show ipv6 ospf**[*process- id*] **database**[*lsa-type* [**adv-router***router-id*]]
Displays OSPF-enabled interfaces.	**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Displays the OSPF neighbor list.	**show ipv6 ospf**[*process- id*] **neighbor**[*interface-type interface-number*[**detail**]| *neighbor-id* |**detail**]
Displays the OSPF routing table.	**show ipv6 ospf** [*process-id*] **route**[**count**]
Displays the summarized route of OSPF redistributed routes.	**showipv6ospf**[*process-id*]**summary-prefix**
Displays the OSPF network topology information.	**show ipv6 ospf**[*process- id*] **topology** [**area***area-id*]
Displays OSPF virtual links.	**show ipv6 ospf** [*process-id*] **virtual-links**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs OSPF events.	**debug ipv6 ospf events** [**abr**|**asbr**|**os**|**nssa**|**router**| **vlink**]
Debugs OSPF interfaces.	**debug ipv6 ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ipv6 ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ipv6 ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ipv6 ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ipv6 ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ipv6 ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

8 Managing Routes

8.1 Overview

The network service module (NSM) manages the routing table, consolidates routes sent by various routing protocols, and selects and sends preferred routes to the routing table. Routes discovered by various routing protocols are stored in the routing table. These routes are generally classified by source into three types:

- Direct route: It is the route discovered by a link-layer protocol and is also called interface route.
- Static route: It is manually configured by the network administrator. A static route is easy to configure and less demanding on the system, and therefore applicable to a small-sized network that is stable and has a simple topology. However, when the network topology changes, the static route must be manually reconfigured and cannot automatically adapt to the topological changes.
- Dynamic route: It is the route discovered by a dynamic routing protocol.

8.2 Applications

Application	Description
Basic Functions of the Static Route	Manually configure a route.
Floating Static Route	Configure a standby route in the multipath scenario.
Load Balancing Static Route	Configure load balancing static routes in the multipath scenario.

8.2.1 Basic Functions of the Static Route

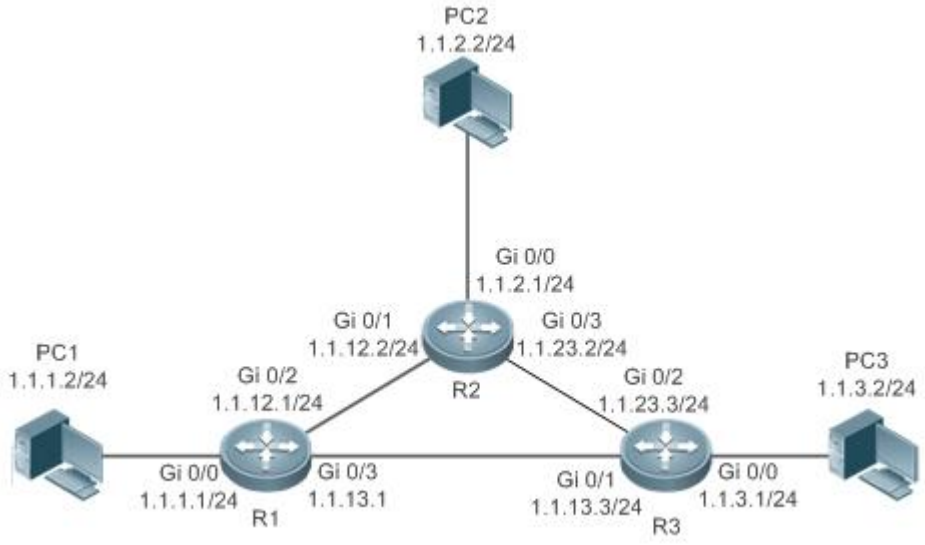
Scenario

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

As shown in Figure 6-1, to implement interworking between PC 1, PC 2, and PC 3, you can configure static routes on R 1, R 2, and R 3.

- On R 1, configure a route to the network segment of PC 2 through R 2, and a route to the network segment of PC 3 through R 3.
- On R 2, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 3 through R 3.
- On R 3, configure a route to the network segment of PC 1 through R 1, and a route to the network segment of PC 2 through R 2.

Figure 6-1



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

8.2.2 Floating Static Route

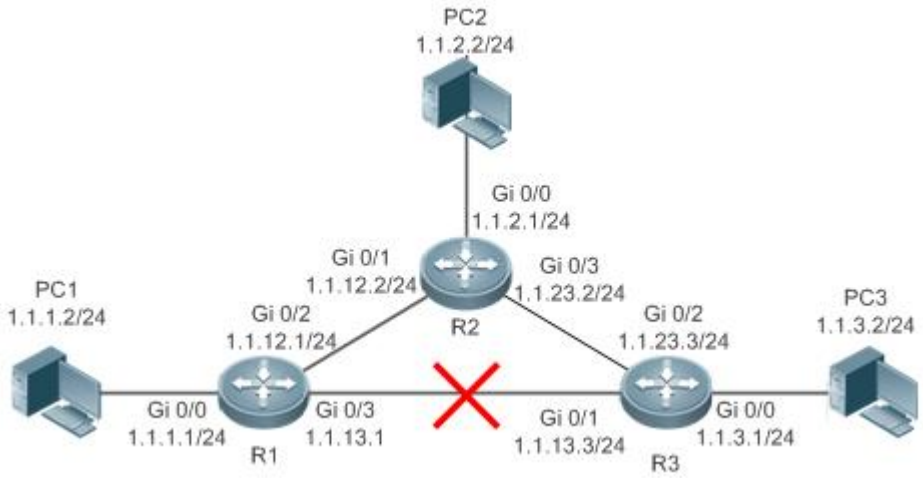
Scenario

If no dynamic routing protocol is configured, you can configure floating static routes to implement dynamic switching of routes to prevent communication interruption caused by the network connection failures.

As shown in Figure 6-2, to prevent communication interruption caused by a line failure between R 1 and R 3, you can configure a floating static route respectively on R 1 and R 3. Normally, packets are forwarded on a path with a small administrative distance. If a link on this path is down, the route is automatically switched to the path with a large administrative distance.

- On R1, configure two routes to the network segment of PC 3, including a route through R 3 (default distance = 1) and a route through R 2 (default distance = 2).
- On R 3, configure two routes to the network segment of PC 1, including a route through R 1 (default distance = 1) and a route through R 2 (default distance = 2).

Figure 6-2



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, and R 3.

8.2.3 Load Balancing Static Route

Scenario

If there are multiple paths to the same destination, you can configure load balancing routes. Unlike floating routes, the administrative distances of load balancingroutes are the same. Packets are distributed among these routes based on the balanced forwarding policy.

As shown in Figure 6-3, load balancing routes are configured respectively on R 1 and R 3 so that packets sent to the network segment of PC 3 or PC 1 are balanced between two routes, including a route through R 2 and a route through R 4.

- On R 1, configure two routes to the network segment of PC 3, including a route through R 2 and a route through R 4.
- On R 3, configure two routes to the network segment of PC 1, including a route through R 2 and a route through R 4.

Figure 6-3

Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R 1, R 2, R 3, and R 4.
- Configure the load balancing policy on R 1 and R 3.

8.3 Features

Feature	Description
Route Computation	Generate a valid route on a device.
Optimal Route Selection	Select an optimal route to forward packets.
Default Route	Forward all packets and help reduce the size of a routing table.

8.3.1 Route Computation

Routing Function

Routing functions are classified into IPv4 and IPv6 routing functions. If the routing functions are disabled, a device is equivalent to a host and cannot forward routes.

Dynamic Route

A dynamic routing protocol learns remote routes and dynamically updates routes by exchanging routes with neighbors. If a neighbor is the next hop of a route and this neighbor fails, the route fails as well.

Static Route

On a network with a simple topology, you can configure only static routes to implement network interworking. Appropriate configuration and use of static routes can improve the network performance and guarantee the bandwidth for important network applications.

Whether a static route is active is computed based on the status of the local interface. When the exit interface of a static route is located at layer 3 (L3) and is in Up status (the link status is Up and the IP address is configured), this route is active and can be used for packet forwarding.

8.3.2 Optimal Route Selection

Administrative Distance

When multiple routing protocols generate routes to the same destination, the priorities of these routes can be determined based on the administrative distance. A smaller administrative distance indicates a higher priority.

Equal-Cost Route

If multiple routes to the same destination have different next hops but the same administrative distance, these routes are mutually equal-cost routes. Packets are distributed among these routes to implement load balancing based on the balanced forwarding policy.

On a specific device, the total number of equal-cost routes is limited. Routes beyond the limit do not participate in packet forwarding.

Floating Route

If multiple routes to the same destination have different next hops and different administrative distances, these routes are mutually floating routes. The route with the smallest administrative distance will be first selected for packet forwarding. If this route fails, a route with a larger administrative distance is further selected for forwarding, thus preventing communication interruption caused by a network line failure.

8.3.3 Default Route

In the forwarding routing table, the route with the destination network segment 0.0.0.0 and the subnet mask 0.0.0.0 is the default route. Packets that cannot be forwarded by other routes will be forwarded by the default route. The default route can be statically configured or generated by a dynamic routing protocol.

Static Default Route

On a L3 switch, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate the default route.

Default Network

The default network is configured to generate a default route. If the **ip default-network** command is configured to specify a network (a classful network, such as a Class A, B, or C network), and this network exists in the routing table, the router will use this network as the default network and the next hop of this network is the default gateway. As the network specified by the **ip default-network** command is a classful one, if this command is used to identify a subnet in a classful network, the router automatically generates a static route of the classful network instead of any default route.

8.4 Configuration

Configuration Item	Description and Command	
Configuring a Static Route	(Mandatory) It is used to configure a static route entry.	
	ip route	Configures an IPv4 static route.
	ipv6 route	Configures an IPv6 static route.
Configuring a Default Route	(Optional) It is used to configure the default gateway.	
	ip default gateway	Configures an IPv4 default gateway on a L2 device.
	ipv6 default gateway	Configures an IPv6 default gateway on a L2 device.
	ip route 0.0.0.0 0.0.0.0 *gateway*	Configures an IPv4 default gateway on a L3 device.
	ipv6 route ::/0 *ipv6-gateway*	Configures an IPv6 default gateway on a L3 device.
	ip default network	Configures an IPv4 default network on a L3 device.
Configuring Route Limitations	(Optional) It is used to limit the number of equal-cost routes and number of static routes, or disable routing.	
	maximum-paths	Configures the maximum number of equal-cost routes.
	ip static route-limit	Configures the maximum number of IPv4 static routes.
	ipv6 static route-limit	Configures the maximum number of IPv6 static routes.
	no ip routing	Disables IPv4 routing.
	noipv6 unicast-routing	Disables IPv6 routing.

8.4.1 Configuring a Static Route

Configuration Effect

- Generate a static route in the routing table. Use the static route to forward packets to a remote network.

Notes

- If the **no ip routing** command is configured on a L3 switch, you cannot configure IPv4 static routes on this switch, and existing IPv4 static routes will also be deleted. Before the device is restarted, reconfiguring the **ip routing** command can recover the deleted IPv4 static routes. After the device is restarted, deleted IPv4 static routes cannot be recovered.

- If the **no ipv6 unicast- routing** command is configured on a L3 switch, you cannot configure IPv6 static routes on this switch, and existing IPv6 static routes will also be deleted. Before the device is restarted, reconfiguring the **ipv6 unicast- routing** command can recover the deleted IPv6 static routes. After the device is restarted, deleted IPv6 static routes cannot be recovered.

Configuration Steps

Configuring a Static IPv4 Route

Configure the following command on an IPv4-enabled router.

Command	**ip route** *networknet-mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**][**weight** *number*] [**description***description-text*] [**disabled** | **enabled**] [**global**]	
Parameter Description	*network*	Indicates the address of the destination network.
	net-mask	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
	global	(Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by *vrf name*.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route** *networknet-maskip-address.*	

Configuring an IPv6 Static Route

Configure the following command on an IPv6-enabled router.

Command	**ipv6 route** *ipv6-prefix*/*prefix-length* { *ipv6-address*] | *interface* [*ipv6-address*] } [*distance*] [**weight***number*]

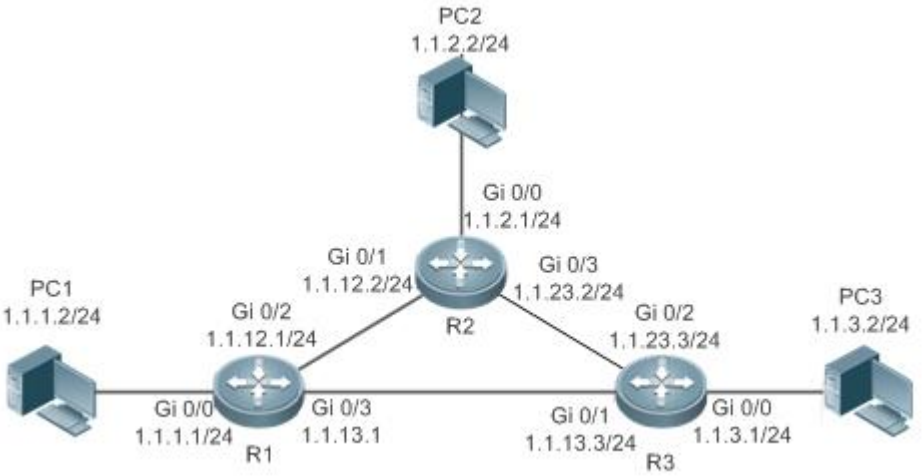
	[**description***description-text*]	
Parameter Description	*ipv6-prefix*	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	prefix-length	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-costroutes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route***ipv6-prefix* / *prefix-lengthipv6-address.*	

Verification

- Run the **show ip route** command to display the IPv4 routing table and check whether the configured IPv4 static route takes effect.
- Run the **show ipv6 route** command to display the IPv6 routing table and check whether the configured IPv6 static route takes effect.

Configuration Example

Configuring Static Routes to Implement Interworking of the IPv4 Network

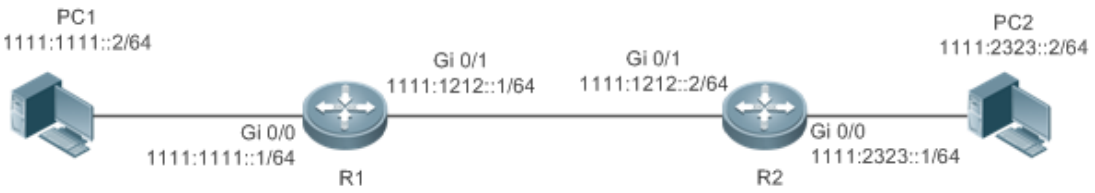
Scenario **Figure 6-4**	
Configuration Steps	● Configure interface addresses on each device.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/3 R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
R3	R3#configure terminal R3(config)#interface gigabitEthernet 0/0

	R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/1 R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/2 R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
	• Configure static routes on each device.
R1	R1#configure terminal R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2 R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
R2	R2#configure terminal R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1 R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
R3	R3#configure terminal R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2 R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
Verification	• Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host.

	S 1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2 S 1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host.
R2	R2# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0 C 1.1.2.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.2.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.2/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.23.2/32 is local host.
R3	R3# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default

```
Gateway of last resort is no set
S      1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2
S      1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2
C      1.1.3.0/24 is directly connected, GigabitEthernet 0/0
C      1.1.3.1/32 is local host.
C      1.1.13.0/24 is directly connected, GigabitEthernet 0/1
C      1.1.13.3/32 is local host.
C      1.1.23.0/24 is directly connected, GigabitEthernet 0/2
C      1.1.23.3/32 is local host.
```

Configuring Static Routes to Implement Interworking of the IPv6 Network

Scenario **Figure 6-5**	
Configuration Steps	● Configure interface addresses on each device.
R1	`R1#configure terminal` `R1(config)#interface gigabitEthernet 0/0` `R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64` `R1(config-if-GigabitEthernet 0/0)# exit` `R1(config)#interface gigabitEthernet 0/1` `R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64`
R2	`R2#configure terminal` `R2(config)#interface gigabitEthernet 0/0` `R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64` `R2(config-if-GigabitEthernet 0/0)# exit` `R2(config)#interface gigabitEthernet 0/1` `R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64`
	● Configure static routes on each device.

R1	R1#configure terminal R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
R2	R2#configure terminal R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
Verification	● Display the routing table.
R1	R1# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:1111::/64 via GigabitEthernet 0/0, directly connected L 1111:1111::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
R2	R2# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C       1111:2323::/64 via GigabitEthernet 0/0, directly connected
L       1111:2323::1/128 via GigabitEthernet 0/0, local host
C       1111:1212::/64 via GigabitEthernet 0/1, directly connected
L       1111:1212::1/128 via GigabitEthernet 0/1, local host
S       1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
```

Common Errors

- The link on the interface is not up.
- No IP address is configured for the interface.

8.4.2 Configuring a Default Route

Configuration Effect

- Generate a default route in the routing table. The default route is used to forward packets that cannot be forwarded by other routes.

Notes

- On a L3 switch, run the **ip route** 0.0.0.0 0.0.0.0 *gateway*or **ipv6 route** ::/0 *ipv6-gateway*command to configure the default gateway.

Configuration Steps

↘ Configuring the IPv4 Default Gateway on a L3 Switch

Command	**ip route 0.0.0.00.0.0.0**{*ip-address* | *interface* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description***description-text*] [**disabled** | **enabled**] [**global**]	
Parameter	**0.0.0.0**	Indicates the address of the destination network.

Description	**0.0.0.0**	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	tag	(Optional) Indicates the tag of the static route. The tag is 0 by default.
	permanent	(Optional) Indicates the flag of the permanent route. The static route is not a permanent route by default.
	weight *number*	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
	disabled /enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
	global	(Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by *vrf name*.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route0.0.0.0 0.0.0.0** *ip-address.*	

Configuring the IPv6 Default Gateway on a L3 Switch

Command	**ipv6 route ::/0** { *ipv6-address* | *interface* [*ipv6-address*] } [*distance*] [**weight***number*] [**description***description-text*]	
Parameter Description	**::**	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC4291.
	0	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added in front of the length.
	Ipv6-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *ipv6-address* is not specified, a static direct route is configured.
	interface	(Optional) Indicates the next-hop exit interface of the static route. You must specify at least one of *ipv6-address* and *interface,* or both of them. If *interface* is not specified, a recursive static direct route is configured. The exit interface is obtained by the next hop in the routing table.
	distance	(Optional) Indicates the administrative distance of the static route. The administrative distance is 1 by default.
	weight *number*	(Optional) Indicates the weight of the static route, which must be specified when you

		configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
	description*description-text*	(Optional) Indicates the description of the static route. By default, no description is configured. *description-text* is a string of one to 60 characters.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route** ::/0 *ipv6-gateway*.	

Configuring the IPv4 Default Network on a L3 Switch

Command	**ip default-network** *network*	
Parameter Description	*network*	Indicates the address of the network. (The network must be a Class A, B, or C network.)
Defaults	By default, no default network is configured.	
Command Mode	Global configuration mode	
Usage Guide	If the network specified by the **ip default-network** command exists, a default route is generated and the next hop to this network is the default gateway. If the network specified by the **ip default-network** command does not exist, the default route is not generated.	

Verification

- On a L3 switch where routing is enabled, run the **show ip route** or **show ipv6 route** command to display the default route.

Configuration Example

Configuring IPv4 Default Routes on L3 Switches to Implement Network Interworking

Scenario Figure 6-6	
Configuration Steps	● Configure IP addresses on L3 devices.
R1	`R1#configure terminal`

	R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit
R1	● Configure an IPv6 default gateway on R 1. R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.1
Verification	● Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is 1.1.12.2 S* 0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1

	C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.1/32 is local host.

8.4.3 Configuring Route Limitations

Configuration Effect

- Limit the number of equal-cost routes and number of static routes, or disable routing.

Notes

N/A

Configuration Steps

Configuring the Maximum Number of Equal-Cost Routes

Command	**maximum-paths***number*	
Parameter Description	*number*	Indicates the maximum number of equal-cost routes. The value ranges from 1 to 64. The actual range varies from products.
Defaults	The default value varies from products.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of next hops in the equal-cost route. In load balancing mode, the number of routes on which traffic is balanced does not exceed the configured number of equal-cost routes.	

Configuring the Maximum Number of IPv4 Static Routes

Command	**ip static route-limit***number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.
Defaults	By default, a maximum of 1, 024 IP static routes can be configured.	
Command Mode	Global configuration mode	
Usage Guide	Run this command to configure the maximum number of IPv4 static routes. If the maximum number of IPv4 static routes is reached, no more IPv4 static route can be configured.	

Configuring the Maximum Number of IPv6 Static Routes

Command	**ipv6 static route-limit***number*	
Parameter Description	*number*	Indicates the upper limit of routes. The value ranges from 1 to 10,000.

Defaults	By default, a maximum of 1,000 IPv6 static routes can be configured.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the maximum number of IPv6 static routes. If the maximum number of IPv6 static routes is reached, no more IPv6 static route can be configured.

Disabling IPv4 Routing

Command	**no ip routing**
Parameter Description	N/A
Defaults	By default, IP routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a voice over IP (VoIP) gateway, the device does not need to use the IPv4 routing function of the RGOS software. In this case, you can disable the IPv4 routing function of the RGOS software.

Disabling IPv6 Routing

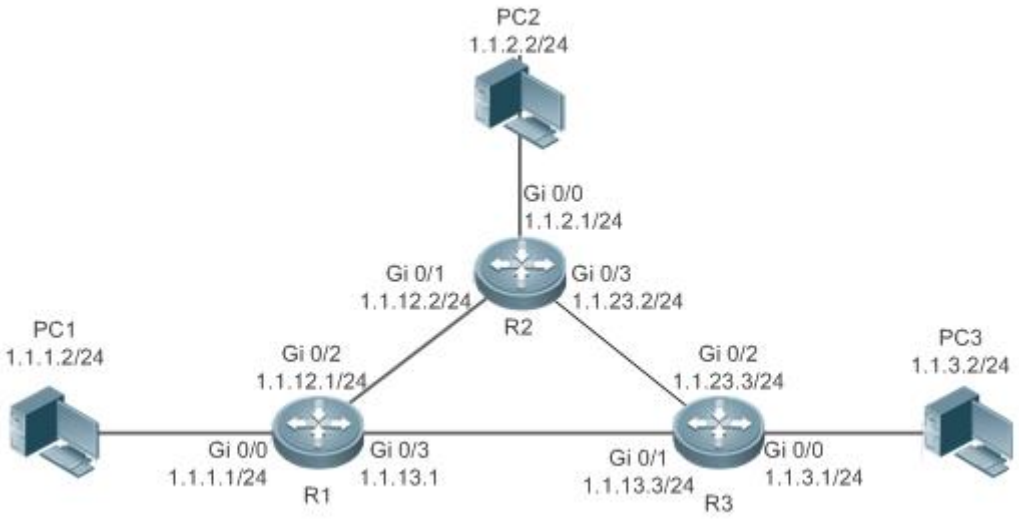
Command	**no ipv6 unicast-routing**
Parameter Description	N/A
Defaults	By default, IPv6 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a VoIP gateway, the device does not need to use the IPv6 routing function of the RGOS software. In this case, you can disable the IPv6 routing function of the RGOS software.

Verification

Run the **show run** command to display the configuration file and verify that the preceding configuration commands exist.

Configuration Example

Configuring at Most Two Static Routing Limitations

Scenario **Figure 6-7**	
Configuration Steps	On R 1, configure the IP addresses, static routes, and maximum number of static routes.
	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0 R1(config-if-GigabitEthernet 0/3)# exit R1(config)#ip route 1.1.3.0 255.255.255.0 1.1.13.3 R1(config)#ip route 1.1.4.0 255.255.255.0 1.1.12.2 R1(config)#ip route 1.1.5.0 255.255.255.0 1.1.12.2 R1(config)#ip static route-limit 2 % Exceeding maximum static routes limit.
Verification	● Check the static routes that really take effect in the routing table.

```
R1(config)# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
S     1.1.3.0/24 [1/0] via 1.1.13.3
S     1.1.4.0/24 [1/0] via 1.1.12.2
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.12.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.13.1/32 is local host.
```

8.5 Monitoring

Displaying

Description	Command
Displays the IPv4 routing table.	**show ip route**
Displays the IPv6 routing table.	**show ipv6route**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs IPv4 route management.	**debug nsm kernel ucast- v4**
Debugs IPv6 route management.	**debug nsm kernel ucast-v6**
Debugs default network management.	**debug nsm kernel default-network**
Debugs internal events of route	**debug nsm events**

management.	
Debugs sending of route management and routing protocol messages.	**debug nsm packet send**
Debugs receiving of route management and routing protocol messages.	**debug nsm packet recv**

9 Configuring FPM

9.1 Overview

The flow platform (FPM) is a platform for the acceleration of packet service processing. Because IP packets have the flow attribute, the FPM provides services with the function to identify the flow attribute of IP packets before service processing, so as to improve service processing efficiency. The FPM is a fundamental platform. It is loaded upon system startup. The configuration commands described in this document are provided to implement FPM configuration and management. In general, the default configuration of the FPM can already meet practical requirements.

The following sections describe the FPM only.

Protocols and Standards

N/A

9.2 Applications

Application	Description
Configuring the packet receiving threshold	A standalone device serves as the gateway to forward packets.
Configuring loose TCP status check	Perform active/standby switchover in the AS environment.

9.2.1 Configuring the Packet Receiving Threshold

Scenario

When the device receives a large number of repeated TCP connection requests in a local area network (LAN), no legitimate connection can be established if the device cannot receive any handshake response packet from the peer. In this case, attacks probably occur. You can perform FPM configuration to restrict the number of TCP connection requests, so as to effectively defend against such attacks.

Protocols

- Enable the strict packet status tracing function on the forwarding device.
- Configure a low TCP-SYN-SENT packet threshold.

9.2.2 Configuring Loose TCP Status Check

Scenario

Loose TCP status check should be configured on the device to prevent flow interruption during active/standby switchover of the device. Then a connection can be established and packets can be forwarded as long as one end sends an ACK packet, so that the connection is not interrupted at all during the active/standby switchover.

Protocols

- Configure loose TCP status check on the backup device.

9.3 Features

Basic Concepts

↘ Flow Entry

A flow entry, as a physical resource for the device to identify and manage all connections of an IP session, records basic information about the current IP session. The corresponding protocols include ICMP, TCP, UDP, and RAWIP.

Overview

Feature	Description
Transparent transmission when the flow table is full	This feature ensures that the existing flows are not interrupted when the flow table is full.
Flow entry aging	This feature reclaims invalid flow entries.
Number of packets permitted in a flow	This feature prevents IP packet flooding attacks.
TCP status tracing	This feature filters out packets on illegitimate TCP connections.
Strict packet status tracing	This feature performs packet threshold check.
Loose TCP status check	This feature allows the establishment of a connection with only ACK packets.

9.3.1 Transparent Transmission of Packets When the Flow Table Is Full

Working Principle

The acceleration of IP service processing relies on a flow table. Flow table resources are configured according to the current product hardware configuration and generally can meet application requirements in an application environment. In some extreme environments, however, flow table resources could be exhausted, causing the failure to establish flows. With this feature, packets are transparently transmitted instead of establishing any flow on wireless products when the flow table is full, and service processing is not accelerated, thereby ensuring that service flows are not interrupted.

9.3.2 Flow Entry Aging

Working Principle

The aging of a flow entry means that the device actively withdraws the flow entry when there is no data exchange in a certain period of time. If a session attack occurs, the flow table will be full, causing the failure to establish sessions. The aging of the flow table is designed to solve this problem. For flow entries of different data types, their aging time shall be set according to actual service requirements. For flows of different service data types, different aging time shall be set according to different states of the flows. For example, the aging time of a TCP flow in SYN status is different from that of a TCP flow in ESTABLISH status. For example again, when a port scanning attack occurs on a network, abundant flow table resources of the system are occupied, and then appropriate aging time can be configured for flows established on these connections according to the states of the flows, so as to effectively reclaim flow entries and avoid flow interruption. Configuring appropriate aging time can help to reduce "useless" flow entries in the flow table while meeting the requirement for exchanging service data flows.

9.3.3 Number of Packets Permitted in a Flow

Working Principle

For each flow in the current status, there is a counter that records the number of packets processed in the flow. An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted to pass in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

9.3.4 TCP Status Tracing

Working Principle

A complete handshake process is required for the establishment of a TCP connection; otherwise, the connection is illegitimate or the packets are attack packets. The FPM needs to trace the states of TCP connections, so as to distinguish flows that are established over TCP session connections in various states and determine whether the connections are legitimate. In some special scenarios such as asymmetrical routing, however, the states of TCP connections cannot be traced and then this function should be disabled.

9.3.5 Packet Threshold for Flows in Various States

Working Principle

For a flow in a certain status established over a connection, there is an upper limit on the number of packets permitted on the legitimate connection. If this upper limit is exceeded, a packet flooding attack probably occurs, occupying the forwarding resources of the system. Therefore, you can configure a packet threshold for flows in various states so as to effectively defend against such attacks.

9.3.6 Loose TCP Status Check

Working Principle

A complete handshake process is required for the establishment of a legitimate TCP connection. In some cases such as active/standby switchover, however, probably a handshake process has been performed for the current TCP connection but only no corresponding information exists. In such cases, the system requires only ACK packets. For this purpose, the FPM provides loose TCP status check.

9.4 Configuration

Configuration	Description and Command	
Configuring the Functions of the FPM	(Optional) It is used to manage FPM.	
	Ip session direct-trans-disable	Disables the function to transparently transmit packets when the flow table is full.
	ip session timeout	Configures the flow entry aging time.
	ip session threshold	Configures the number of packets that can be received for each flow in a certain status.
	ip session tcp_state-inspection-enable	Enables the TCP status tracing function.
	ip session track-state-strictly	Configures packet threshold for flows in various states.
	ip session tcp-loose	Enables the loose TCP status transition check function.

9.4.1 Disabling Transparent Transmission of Packets When the Flow Table Is Full

Networking Requirements

- For some special services such as network address translation (NAT) applied on wireless products, the FPM should not allow the transparent transmission of packets without flow establishment.

Notes

- Currently this function is available on wireless products only.
- By default, packets can be transparently transmitted without flow establishment when the flow table is full.

Configuration Steps

- Optional configuration.

- By default, packets can be transparently transmitted without flow establishment when the flow table is full. You can use the **ip session direct-trans-disable** command to disable the function.

Command	**ip session direct-trans-disable**
Parameter Description	
Defaults	Packets can be transparently transmitted without flow establishment when the flow table is full.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to enable the transparent transmission function.

Verification

- Use the **show run** command to check whether the configuration includes **ip session direct-trans-disable**. If no, the transparent transmission function is enabled.

Configuration Example

Scenario	If the NAT service is required on the current wireless device, you need to disable the transparent transmission function because the NAT service does not allow the transparent transmission of IP packets without flow establishment.
Configuration Steps	Disable transparent transmission of packets without flow establishment when the flow table is full.
	`Ruijie# configure terminal` `Ruijie(config)# ip session direct-trans-disable`
Verification	Use the **show run** command to verify that the configuration includes **ip session direct-trans-disable**.

Common Errors

N/A

9.4.2 Configuring the Flow Entry Aging Time

Networking Requirements

- Reasonably make use of system flow table resources so as to reduce "useless" flow entries in the flow table and meet the requirement for exchanging service data flows.

Notes

- There is a default aging time upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- Because a certain time is required before the system detects the corresponding flow, the actual aging time is slightly later than the configured aging time.

Configuration Steps

↘ Configuring the Aging Time

- Optional configuration.
- By default, a flow entry ages within the default aging time. If the default aging time does not meet the requirement, you can use the **ip session timeout** command to change it. The longer the aging time, the longer the time-to-live (TTL) of the flow entry.
- Perform this configuration on the corresponding forwarding device.

Command	**ip session timeout** {**icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin-wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established**} { *num* }
Parameter Description	**icmp-closed**: Sets the aging time of ICMP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **icmp-connected**: Sets the aging time of ICMP flows in connected status, which is 10 seconds by default and ranges from 5 to 120. **icmp-started**: Sets the aging time of ICMP flows in started status, which is 10 seconds by default and ranges from 5 to 120. **rawip-closed**: Sets the aging time of RAWIP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **rawip-connected**: Sets the aging time of RAWIP flows in connected status, which is 300 seconds by default and ranges from 10 to 300. **rawip-established**: Sets the aging time of RAWIP flows in established status, which is 300 seconds by default and ranges from 10 to 600. **rawip-started**: Sets the aging time of RAWIP flows in started status, which is 300 seconds by default and ranges from 10 to 300. **tcp-close-wait**: Sets the aging time of TCP flows in tcp-close-wait status, which is 60 seconds by default and ranges from 10 to 120. **tcp-closed**: Sets the aging time of TCP flows in tcp-closed status, which is 10 seconds by default and ranges from 5 to 20. **tcp-established**: Sets the aging time of TCP flows in tcp-established status, which is 1,800 seconds by default and ranges from 300 to 604,800. **tcp-fin-wait1**: Sets the aging time of TCP flows in tcp-fin-wait1status, which is 60 seconds by default and ranges from 10 to 120. **tcp-fin-wait2**: Sets the aging time of TCP flows in tcp-fin-wait2status, which is 60 seconds by default and ranges from 10 to 120. **tcp-syn-sent**: Sets the aging time of TCP flows in tcp-syn-sent status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn_sent2**: Sets the aging time of TCP flows in tcp-syn_sent2 status, which is 10 seconds by default and ranges from 5 to 30. **tcp-syn-receive**: Sets the aging time of TCP flows in tcp-syn-receive status, which is 10 seconds by default and ranges from 5 to 30. **tcp-time-wait**: Sets the aging time of TCP flows in tcp-time-wait status, which is 10 seconds by

	default and ranges from 5 to 60. **udp-closed**: Sets the aging time of UDP flows in closed status, which is 10 seconds by default and ranges from 5 to 60. **udp-connected**: Sets the aging time of UDP flows in connected status, which is 30 seconds by default and ranges from 10 to 300. **udp-established**: Sets the aging time of UDP flows in established status, which is 600 seconds by default and ranges from 120 to 600. **udp-started**: Sets the aging time of UDP flows in started status, which is 10 seconds by default and ranges from 10 to 300. **num**: Sets the aging time
Defaults	Default values apply.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the commands to restore the default aging time.

Verification

- Use the **show run** command to check whether the configuration includes **ip session timeout**. If no, the default aging time applies.

Configuration Example

Scenario	If there are a large number of UDP-established flows which occupy a great space of the flow table on the current forwarding device, you can shorten the aging time of the UDP-established flows to improve aging efficiency.
Configuration Steps	Set the aging time of flows in udp-established status to 120 seconds.
	`Ruijie# configure terminal` `Ruijie(config)# ip session timeout udp-established 120`
Verification	The aging time should be 120 seconds. Use the **show run** command to verify that the configuration contains the following item: `ip session  timeout udp-established 120` This indicates that the aging time is 120 seconds.

Common Errors

-

9.4.3 Configuring the Number of Packets Permitted in a Flow

Networking Requirements

- An attacker may send a large number of packets of a certain type to wage a traffic attack, in which case other types of packets cannot be processed in time. You can configure the number of packets permitted in a flow in a certain status, so as to solve this problem and meet the requirement for exchanging service data flows.

Notes

- There is a default packet count upon system initialization, which can meet practical requirements in most scenarios. Therefore, the configuration is optional.
- The check function here is disabled by default. To enable the check function, you need to configure packet threshold check for flows in various states first.

Configuration Steps

- Optional configuration.
- By default, a flow is judged according to the default number of packets permitted to pass in the flow. If the default number of packets permitted to pass does not meet the requirement, you can use the **ip session threshold** command to change the number of packets allowed to pass in the corresponding flow. The greater the value, the more packets permitted to pass in the flow.
- Perform this configuration on each forwarding device as necessary.

Command	**ip session threshold** {icmp-closed | **icmp-started** | rawip-closed | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed** } { *num* }
Parameter Description	**icmp-closed**: Sets the number of packets permitted to pass in each ICMP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **icmp-started**: Sets the number of packets permitted to pass in each ICMP flow in started status, which is 300 by default and ranges from 5 to 2,000,000,000. **rawip-closed**: Sets the number of packets permitted to pass in each RAWIP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. **tcp-syn-sent**: Sets the number of packets permitted to pass in each TCP flow in syn-send status, which is 10 by default and ranges from 10 to 2,000,000,000. **tcp-syn-receive**: Sets the number of packets permitted to pass in each TCP flow in syn-receive status, which is 20 by default and ranges from 5 to 2,000,000,000. **tcp-closed**: Sets the number of packets permitted to pass in each TCP flow in closed status, which is 20 by default and ranges from 5 to 2,000,000,000. **udp-closed**: Sets the number of packets permitted to pass in each UDP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000. *num*: Sets the number of packets permitted to pass
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the command to restore the default number of packets permitted to pass.

Verification

- Use the **show run** command to check whether the configuration includes **ip session threshold**. If no, the default values about the number of packets permitted to pass apply.

Configuration Example

Scenario	When a large number of ping packets exist on a network, a flooding attack probably occurs. You can

	configure the number of packets permitted to pass in each ICMP flow in icmp-started status, so as to deny such ping packets.
Configuration Steps	Set the number of packets permitted to pass in each ICMP flow in icmp-started status to 10.
	`Ruijie# configure terminal` `Ruijie(config)# ip session threshold icmp-started 10`
Verification	The number should be 10. Use the **show run** command to verify that the configuration contains the following item: `ip session threshold icmp-started 10` This indicates that the number of packets permitted to pass in each ICMP flow in icmp-started status is 10.

Common Errors

-

9.4.4 Enabling the TCP Status Tracing Function

Networking Requirements

- The TCP status tracing function needs to be enabled on corresponding wireless products.

Notes

- By default, the TCP status tracing function is disabled on wireless products.

Configuration Steps

- Optional configuration.
- By default, the TCP status tracing function is disabled. You can use the **ip session tcp-state-inspection-enable** command to enable.

Command	**ip session tcp-state-inspection-enable**
Parameter Description	
Defaults	The TCP status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the TCP status tracing function to the default.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-state-inspection-enable**. If no, the TCP status tracing function is disabled.

Configuration Example

Scenario	The TCP status tracing function needs to be enabled on the current wireless forwarding device.
Configuration	Enable the TCP status tracing function on the device.

Steps	
	Ruijie# configure terminal Ruijie(config)# ip session tcp-state-inspection-enable
Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-state-inspection-enable**.

Common Errors

-

9.4.5 Configuring Packet Threshold Check for Flows in Various States

Networking Requirements

- Perform this configuration to enable the packet threshold check function and disable the current flow when packets are unreachable.

Notes

-

Configuration Steps

- Optional configuration.
- You can use the **ip session track-state-strictly** command to enable the strict packet status tracing function.
- The packet threshold check function needs to be enabled in a scenario such as the scenario where attacks are waged using a certain type of packet.

Command	**ip session track-state-strictly**
Parameter Description	
Defaults	The strict packet status tracing function is disabled.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session track-state-strictly**. If no, the strict packet status tracing function is disabled.

Configuration Example

Scenario	If ICMP flooding attacks occur in the current network environment, packet threshold check is needed. In this case, perform this configuration to enable the packet threshold check function.

Configuration Steps	Enable the strict packet status tracing function on the forwarding device.
	Ruijie# configure terminal Ruijie(config)# ip session track-state-strictly
Verification	Use the **show run** command to verify that the configuration includes **ip session track-state-strictly**.

Common Errors

-

9.4.6 Configuring Loose TCP Status Check

Networking Requirements

- A flow can be directly established with only ACK packets.

Notes

- By default, the establishment of a flow with an ACK packet.
- This configuration is optional.

Configuration Steps

- Optional configuration.
- By default, the loose TCP status check function is enabled.
- The loose TCP status check function is required on the standby device in a scenario such as active/standby switchover.

Command	**ip session tcp-loose**
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of this command to restore the default configuration.

Verification

- Use the **show run** command to check whether the configuration includes **ip session tcp-loose**. If no, the loose TCP status check function is disabled.

Configuration Example

Scenario	Active/standby switchover is required in the current environment. Perform this configuration on the backup device.
Configuration Steps	Enable the loose TCP status check function on the device.
	Ruijie# configure terminal Ruijie(config)# ip session tcp-loose

Verification	Use the **show run** command to verify that the configuration includes **ip session tcp-loose**.

Common Errors

-

9.5 Monitoring

Clearing

If you run the **clear** command while the device is operating, services may be interrupted arising from the loss of important information.

Function	Command
Clears counters about the IPv4 packets.	**clear ip fpm counters**
Clears counters about the IPv6 packets.	**clear ip v6fpm counters**

Displaying

Function	Command
Displays the counters about the IPv4 packets	**show ip fpm counters**
Displays the counters about the IPv6 packets	**show ip v6fpm counters**
Displays IPv4 packet flow information	**show ip fpm flows**
Displays IPv4 packet flow information except specific IPv4 packet flows	**show ip fpm flows filter**
Displays IPv6 packet flow information	**show ip v6fpm flows**
Displays IPv6 packet flow information except specific IPv6 packet flows	**show ip v6fpm flows filter**
Displays IPv4 flow statistics	**show ip fpm statistics**
Displays IPv6 flow statistics	**show ip v6fpm statistics**

Multicast Configuration

1. Configuring IP Multicasting
2. Configuring IGMP
3. Configuring PIM-DM
4. Configuring PIM-SM
5. Configuring IGMP Snooping

1 Configuring IP Multicasting

1.1 Overview

IP multicasting is abstracted hardware multicasting and an extended multicast routing protocol on the standard IP network layer.

In traditional IP transmission, only one host can send packets to a single host (unicast communication) or all hosts (broadcast communication). However, the multicast technology provides the third choice: a host can send packets to certain specified hosts.

IP multicasting is applicable to one-to-many multimedia applications.

1.2 Applications

Application	Description
PIM-DM Applications	The PIM-DM multicast service is provided on the same network.
PIM-SM Applications	The PIM-SM multicast service is provided on the same network.

1.2.1 PIM-DM Applications

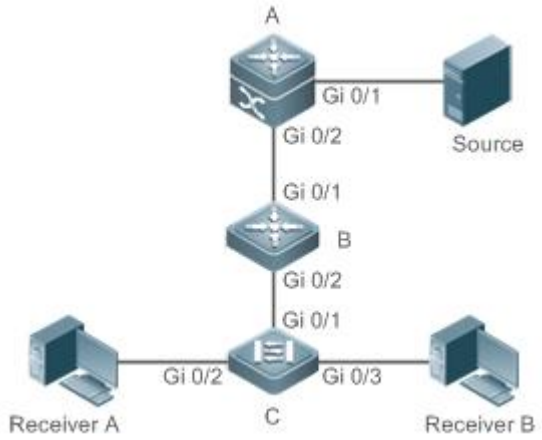
Scenario

The PIM-DM multicast service is provided on the same network.

As shown in Figure 1-1:

- A multicast source sends a multicast packet, and receiver A and receiver B on the same network receive the multicast packet.

Figure 1-1



Remarks	A and B are layer-3 devices and C is a layer-2 access device. Source is connected to the Gi 0/1 interface of A, and receiver A and receiver B are connected to the Gi 0/2 and Gi 0/3 interfaces of C.

Deployment

- Run the Open Shortest Path First (OSPF) protocol on the same network to implement unicast routing.
- Run PIM-DM on the same network to implement multicast routing.
- Run the Internet Group Membership Protocol (IGMP) in a user host network segment to implement group member management.

1.2.2 PIM-SM Applications

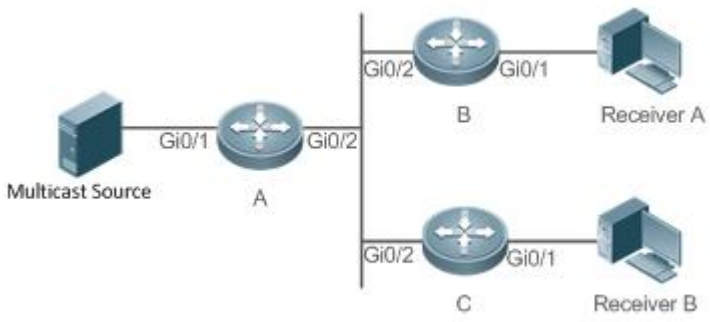
Scenario

The PIM-SM multicast service is provided on the same network.

As shown in Figure 1-2:

- A multicast source sends a multicast packet, and receiver A and receiver B on the same network receive the multicast packet.

Figure 1-2



Remarks	A, B, and C are layer-3 routers. The multicast source is connected to the Gi 0/1 interface of A, receiver B is connected to the Gi 0/1 interface of B, and receiver B is connected to the Gi 0/1 interface of C.

Deployment

- Run OSPF on the same network to implement unicast routing.
- Run PIM-SM on the same network to implement multicast routing.
- Run IGMP in a user host network segment to implement group member management.

1.3 Features

Basic Concepts

↘ PIM Routers and PIM Interfaces

Routers enabled with PIM are called PIM routers. Interfaces enabled with PIM protocol are called PIM interfaces.

Multicast packets are forwarded on PIM routers. The PIM interfaces for receiving multicast packets are called upstream interfaces, and the PIM interfaces for sending multicast packets are called downstream interfaces.

The network segments where upstream interfaces are located are called upstream network segments. The network segments where downstream interfaces are located are called downstream network segments.

↘ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On certain PIM interfaces, borders are configured to divide a large PIM network into multiple PIM domains. Borders may reject specified multicast packets or limit transmission of PIM messages.

↘ Multicast Distribution Tree, DR and RP

Multicast packets are transmitted from one point to multiple points. The forwarding path is in a tree structure. This forwarding path is called a multicast distribution tree (MDT) and has the following types:

- Rendezvous Point Tree (RPT): The RP is regarded as the root and the designated router (DR) that connects group members is regarded as a leaf.
- Shortest Path Tree (SPT): The DR that connects multicast sources is regarded as the root, and RP or DR that connects group members is regarded as a leaf.

The DR and RP are functional roles for a PIM router.

- The RP collects multicast sources and group member information on the network.
- The DR that connects multicast sources reports multicast source information to the RP. The DR that connects group members reports group member information to the RP.

(*,G) and (S,G)

- (*,G): Packets sent from any source to group G, routing entries corresponding to the packets, and forwarding path (RPT) corresponding to the packets.
- (S,G): Packets sent from source S to group G, routing entries corresponding to the packets, and forwarding path (SPT) corresponding to the packets.

ASM and SSM

PIM-SM supports the following multicast models that are applicable to different multicast address segments:

- Any-Source Multicast (ASM): In the ASM model, user hosts cannot select multicast sources. User hosts join a group and receive packets sent from all sources to the group.
- Source-Specific Multicast (SSM): In the SSM model, user hosts can select multicast sources. User hosts specify source addresses when joining a group and receive only packets sent from specified sources to the group.

SSM model requirements: User hosts must know the multicast source address in advance using other network services so that the hosts can select multicast sources.

Overview

Feature	Description
Configuring Basic Functions of IP Multicasting	Creates a PIM network and provides data sources and user terminals on the network with the IPv4 multicast service.
Configuring a TTL Threshold	Configures a TTL threshold for an interface, that is, the minimum TTL value of multicast packets allowed on an interface.
Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	Limits the number of entries that can be added to the multicast routing table.

Feature	Description
Configuring an IP Multicasting Border	Configures an interface as a multicast border for a specified group.
Configuring an IP Multicasting Static Route	Allows the multicast forwarding path to be different from the unicast path.
Configuring Layer-2 Direction Control for Multicast Streams	Allows a specified multicast stream to be configured with multiple commands, that is, to be configured with multiple ports that can forward the stream. Once direction control is configured for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream.
Configuring RPF Route Selection Based on the Longest Match Rule	Selects an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table according to RPF rules. Among these three routes, the one with the longest match mask is selected as the RPF route.
Configuring an RPF Proxy	Configures an RPF proxy to request PIM-SM to send a Join message with RPF vector to establish an SPT.
Configuring Multicast Non-Stop Forwarding Parameters	During normal running, SSP synchronizes the hardware multicast forwarding table to the management board in real time. After the management board is switched, the command for configuring the multicast control plane of the original slave management board is loaded, and the multicast protocol (such as PIM-SM or IGMP Snooping) re-converges. The multicast non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of the multicast protocol.
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	Deletes the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

1.3.1 Configuring Basic Functions of IP Multicasting

Create a PIM network and provide data sources and user terminals on the network with the IPv4 multicast service.

Working Principle

A device maintains the routing table for forwarding multicast packets through multicast routing protocols (such as PIM-DM or PIM-SM) and learns the states of group members in the directly connected network segment through IGMP. A host sends IGMP Report messages to join a specified IGMP group.

Related Configuration

↘ **Enabling IPv4 Multicast Routing**

By default, IPv4 multicast routing is disabled.

Run **ip multicast-routing** to enable IPv4 multicast routing.

↘ Configuring IP Multicasting on an Interface

By default, IP multicasting is disabled on an interface.

Run **ip pim spase-mode** or **ip pim dense-mode** to enable IP multicasting on an interface.

1.3.2 Configuring a TTL Threshold

Configure a TTL threshold for an interface, that is, the minimum TTL value of multicast packets allowed on an interface.

Working Principle

Configure a TTL threshold for an interface and check the TTL values of multicast packets. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded.

Related Configuration

↘ Configuring a TTL Threshold

By default, the TTL threshold of an interface is 0.

Run **ip multicast ttl-threshold** *ttl-value* to change the TTL threshold of an interface. The value ranges from 0 to 255.

A larger value of *ittl-value* means a larger TTL value of multicast packets to be forwarded.

1.3.3 Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Each multicast data packet received on the device maintains a corresponding IP multicast route forwarding entry. However, excess multicast routing entries may exhaust device memory and deteriorate device performance. You can limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Working Principle

The number of entries in the IP multicasting routing table is limited based on the actual network and service performance requirements to ensure device performance.

Related Configuration

↘ Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

By default, a maximum of 1024 entries can be added to an IP multicast routing table.

Run **ip multicast route-limit** *limit* [*threshold*] to change the number of entries that can be added to the IP multicasting routing table. The value ranges from 1 to 65536.

A larger value of *limit* means a larger number of entries that can be added to the IP multicasting routing table.

1.3.4 Configuring an IP Multicasting Border

Configure an IP multicasting border to specify the transmission range of multicast packets.

Working Principle

An IP multicasting border is configured to specify the transmission range of multicast packets. When an IP multicasting border is configured on an interface, this interface cannot forward or receive multicast packets, including those sent from the local host.

Related Configuration

↘ Configuring an IP Multicasting Border

By default, no IP multicasting border is configured.

Run **ip multicast boundary** *access-list* [**in** | **out**] to configure an IP multicasting border.

1.3.5 Configuring an IP Multicasting Static Route

Configure an IP multicasting static route to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Working Principle

An RPF check is performed once multicast packets are forwarded. An IP multicasting static route can be configured to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Related Configuration

↘ Configuring an IP Multicasting Static Route

By default, no IP multicasting static route is configured.

Run **ip mroute** *source-address mask* [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*] to configure an IP multicasting static route.

1.3.6 Configuring RPF Route Selection Based on the Longest Match Rule

Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table and select the one with the longest match mask as the RPF route from the three optimal routes.

Working Principle

A multicast static route, an MBGP route, and a unicast route that can be used for RPF check are selected respectively from the multicast static routing table, MBGP routing table, and unicast routing table according to RPF rules.

- If the longest match rule is used, the route with the longest match mask is selected as the RPF route. If the three routes have the same mask, the one with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.
- Otherwise, the one with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

Related Configuration

↘ Configuring RPF Route Selection Based on the Longest Match Rule

By default, the route with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

Run **ip multicast rpf longest-match** to configure RPF route selection based on the longest match rule.

1.3.7 Configuring Forced Forwarding of Multicast Packets by Software

IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Working Principle

After configuring this function, all IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Related Configuration

↘ Configuring Forced Forwarding of CPU-destined IPv4 Multicast Data Packets by Software

This function is disabled by default.

Run **msf force-forwarding** to enable IPv4 multicast data packets destined for the CPU to be forcedly forwarded by software.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of IP Multicasting	⚠ (Mandatory) It is used to configure the multicast service.	
	ip multicast-routing	Enables the IPv4 multicast routing function.
Configuring a TTL Threshold	⚠ Optional.	
	ip multicast ttl-threshold *ttl-value*	Configures a TTL threshold for an interface.
Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	**ip multicast route-limit** *limit* [*threshold*]	Limits the number of entries that can be added to the multicast routing table.

Configuring an IP Multicasting Border	**ip multicast boundary** *access-list* [**in** | **out**]	Configures an interface as a multicast border for a specified group.
Configuring an IP Multicasting Static Route	**ip mroute** *source-address mask* [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*]	Configures an IP multicasting static route.
Configuring RPF Route Selection Based on the Longest Match Rule	**ip multicast rpf longest-match**	Configures RPF route selection based on the longest match rule.
Configuring Forced Forwarding of Multicast Packets by Software	**msf force-forwarding**	Configures forced forwarding of multicast packets by software.

1.4.1 Configuring Basic Functions of IP Multicasting

Configuration Effect

- Create a PIM network and provide data sources and user terminals on the network with the IPv4 multicast service.

Notes

- A PIM network needs to use existing unicast routes on the network. Therefore, IPv4 routes must be configured on the network.

Configuration Steps

↘ Enabling IPv4 Multicast Routing

- Mandatory.
- IPv4 multicast routing should be enabled on each router unless otherwise specified.

↘ Enabling IP Multicasting for an Interface

- Mandatory.
- IP multicasting protocol should be enabled on interfaces unless otherwise specified:

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups.

- Check whether the user hosts can successfully receive packets from each group.

Related Commands

↘ Enabling IPv4 Multicast Routing

Command	**ip multicast-routing**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	-

Configuring IP Multicasting

For IGMP configuration, see the IGMP section.

For PIM-DM configuration, see the PIM-DM section.

For PIM-SM configuration, see the PIM-SM section.

For DVMRP configuration, see the DVMRP section.

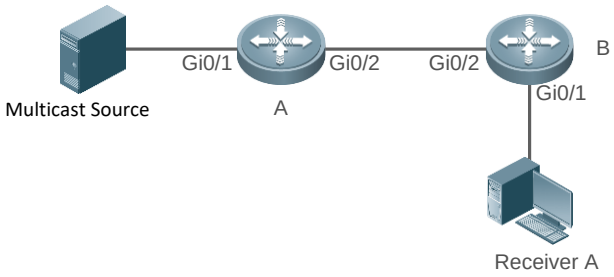
After layer-3 multicasting is enabled in the private VLAN and super VLAN and a multicast source exists in the sub-VLAN, an extra entry whose ingress is the sub-VLAN into which the multicast stream enters needs to be copied due to the validity check during multicast forwarding. This results in occupation of one more multicast hardware entry and one less in the multicast capacity.

Displaying Information About the Multicast Forwarding Table

Command	**show ip mroute** [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]
Parameter Description	*group-or-source-address*: Specifies a group address or source address. *group-or-source-address*: Specifies a group address or source address. **dense**: Displays the core entry of PIM-DM multicast. **sparse**: Displays the core entry of PIM-SM multicast. **summary**: Displays summary information about multicast routing entries. **count**: Displays counting information about multicast routing entries.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	The three parameters are optional, and the source address and group address must be specified simultaneously. When no source address or group address is specified, all MFC entries are displayed. When only the source address and group address are specified, MFC entries of the source address and group address are displayed.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Supporting PIM-DM

Scenario **Figure 1-3**	
Configuration Steps	● Configure an IPv4 unicast routing protocol (such as OSPF) on a router. ● Enable IPv4 multicast routing on all routers. ● Enable PIM-DM on device interconnection interfaces and interfaces for connecting user hosts and multicast sources.
A	`A# configure terminal` `A(config)# ip multicast-routing` `A(config)# interface GigabitEthernet 0/1` `A(config-if)# ip pim dense-mode` `A(config-if)# exit` `A(config)# interface GigabitEthernet 0/2` `A(config-if)# ip pim dense-mode` `A(config-if)# exit`
B	`B# configure terminal` `B(config)# ip multicast-routing` `B(config)# interface GigabitEthernet 0/1` `B(config-if)# ip pim dense-mode` `B(config-if)# exit` `B(config)# interface GigabitEthernet 0/2` `B(config-if)# ip pim dense-mode` `B(config-if)# exit`
Verification	Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G. ● Check multicast packets received by receiver A. Receiver A should be able to receive multicast packets from G. ● Check multicast forwarding tables on A and B.

A	A# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:01:55, stat expires 00:02:19 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)
B	B# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:35, stat expires 00:02:55 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)

Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.
- IP multicasting is not enabled on an interface.

1.4.2 Configuring a TTL Threshold

Configuration Effect

- Configure a TTL threshold for an interface and check the TTL values of multicast packets. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Set a TTL threshold on PIM router interfaces unless otherwise specified.

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups.

- Set a TTL threshold to a value that is larger than the TTL value of the multicast packet on the PIM router interface directly connected to the user host and check whether the user can receive the multicast packet.

Related Commands

↘ Configuring a TTL Threshold

Command	**ip multicast ttl-threshold** *ttl-value*
Parameter Description	*ttl-value*: Specifies a TTL threshold for an interface. The value ranges from 0 to 255. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	A multicast-enabled device can retain a TTL threshold for each interface. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded. A TTL threshold takes effect only for multicast frames and must be configured on layer-3 interfaces.

Configuration Example

↘ Creating the IP Multicast Service on the IPv4 Network and Configuring a TTL Threshold

Scenario **Figure 1-4**	
Configuration Steps	● Configure the basic functions of IP multicasting. (Omitted) ● Configure the TTL threshold as 100 on the Gi 0/2 interface of device A.
A	`A# configure terminal` `A(config)#int gigabitEthernet 0/2` `A(config-if-GigabitEthernet 0/2)#ip multicast ttl-threshold 100` `A(config-if-GigabitEthernet 0/2)# exit`
Verification	Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G. ● Configure the TTL threshold as 100 on the Gi 0/2 interface of device A, which is larger than the TTL value of the multicast packet. ● Check the difference between the route forwarding entries before and after the TTL threshold is configured.
Before Configuring the TTL Threshold	`A# show ip mroute` `IP Multicast Routing Table` `Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,` `R - RPT, S - SPT, s - SSM Group` `Timers: Uptime/Stat Expiry` `Interface State: Interface (TTL)` `(192.168.1.100, 233.3.3.3), uptime 00:00:08, stat expires 00:03:29` `Owner PIMDM, Flags: TFS` `Incoming interface: GigabitEthernet 0/1` `Outgoing interface list:`

	GigabitEthernet 0/2 (1)
After Configuring the TTL Threshold	A# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed, R - RPT, S - SPT, s - SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:01, stat expires 00:03:29 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (100)

1.4.3 Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Configuration Effect

- Each multicast data packet received on the device maintains a corresponding IP multicast route forwarding entry. However, excess multicast routing entries may exhaust device memory and deteriorate device performance. You can limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Verification

Send N groups of multicast packets from the multicast source on the network, configure user hosts to join the groups, configure the number of entries that can be added to the IP multicast routing table as N-1, and check whether the multicast packet received by the user host is that of the N-1 group.

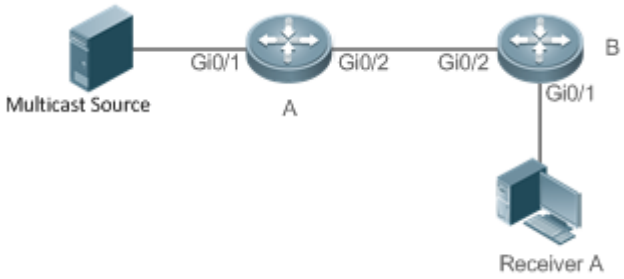
Related Commands

Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Command	**ip multicast route-limit** *limit* [*threshold*]
Parameter Description	*limit*: Specifies the number of entries in the multicast routing table. The value ranges from 1 to 65536. The default value is 1024. *threshold*: Specifies the number of entries in the multicast routing table that triggers the warning message. The default value is 65536.
Command Mode	Global configuration mode
Usage Guide	Due to limitations on hardware resources, routing entries that exceed the range permitted by hardware can be forwarded only by software, deteriorating the performance.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Scenario **Figure 1-5**	
Configuration Steps	● Configure basic the functions of IP multicasting. (Omitted) ● Configure the number of entries that can be added to the multicast routing table on device B as 2.
B	`B# configure terminal` `B(config)# ip multicast route-limit 2`
Verification	Enable the multicast source (192.168.1.100) to send packets to G1 (233.3.3.1), G2 (233.3.3.2), and G3 (233.3.3.3).Enable receiver A to join G1, G2, and G3. ● Check multicast packets received by receiver A. Receiver A should be able to receive multicast packets from two groups among G1, G2, and G3. ● Check multicast routing entries on A and B. ● When the number of entries in the IP multicasting routing table reaches the upper threshold, a prompt message is displayed.

A

```
A# show ip mroute


IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)


(192.168.1.100, 233.3.3.1), uptime 00:00:06, stat expires 00:03:24
Owner PIMDM, Flags: TFS
  Incoming interface: GigabitEthernet 0/1
  Outgoing interface list:
     GigabitEthernet 0/2 (1)

(192.168.1.100, 233.3.3.2), uptime 00:00:05, stat expires 00:03:25
Owner PIMDM, Flags: TFS
  Incoming interface: GigabitEthernet 0/1
  Outgoing interface list:
     GigabitEthernet 0/2 (1)

(192.168.1.100, 233.3.3.3), uptime 00:00:00, stat expires 00:03:30
Owner PIMDM, Flags: TFS
  Incoming interface: GigabitEthernet 0/1
  Outgoing interface list:
     GigabitEthernet 0/2 (1)
```

B

```
B# show ip mroute


IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed,
      R - RPT, S - SPT, s - SSM Group
Timers: Uptime/Stat Expiry
```

	Interface State: Interface (TTL) (192.168.1.100, 233.3.3.1), uptime 00:01:13, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1) (192.168.1.100, 233.3.3.3), uptime 00:06:08, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)
	When the number of entries in the IP multicasting routing table reaches the upper threshold, a prompt message is displayed. B#*Dec 26 10:43:07: %MROUTE-4-ROUTELIMIT: IPv4 Multicast route limit 2 exceeded - VRF default.

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.4.4 Configuring an IP Multicasting Border

Configuration Effect

- Configure an IP multicasting border to specify the transmission range of multicast packets.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure an IP multicasting border on PIM router interfaces unless otherwise specified.

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups. Configure an IP multicasting border on the PIM router interface connected to the user host and check whether the user can receive the multicast packet.

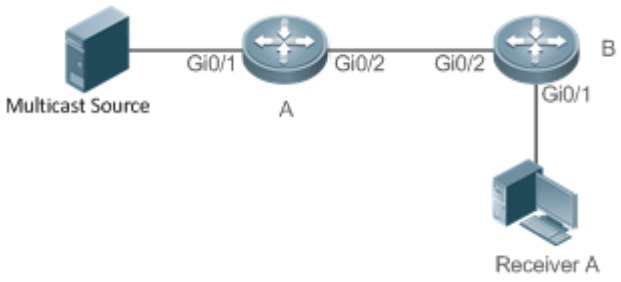
Related Commands

Enabling IPv4 Multicast Routing

Command	**ip multicast boundary** *access-list* [**in** | **out**]
Parameter Description	*access-list*: Indicates the group address range defined by ACL. ***in***: Indicates that the IP multicasting border takes effect in the incoming direction of the multicast stream. ***out***: Indicates that the IP multicasting border takes effect in the outgoing direction of the multicast stream.
Command Mode	Interface configuration mode
Usage Guide	After this command is executed, IGMP and PIM-SM packets in the group range are filtered on this interface and multicast data streams are not going in and out through this interface. The ACL associated with this command can be a standard ACL or an extended ACL. For extended ACLs, only the destination address is matched and the source address is matched.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Configuring an IP Multicasting Border

Scenario **Figure 1-6**	
Configuration Steps	● Configure the basic functions of IP multicasting. (Omitted) ● Configure an ACL on device A. ● Configure an IP multicasting border on the Gi 0/1 interface of device A.
A	`A# configure terminal` `A(config)#ip access-list standard ip_multicast` `A(config-std-nacl)#deny any` `A(config-std-nacl)#exit` `A(config)# interface GigabitEthernet 0/1` `A(config-if-GigabitEthernet 0/1)#ip multicast boundary ip_multicast A` `A(config-if-GigabitEthernet 0/1)# exit`

Verification	Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G. ● Run **debug ip pim sparse-mode events**.
A	`A# debug ip pim sparse-mode events` `Jan 1 20:58:34: %7: VRF(0): No cache message: src 192.168.1.100 for 233.3.3.3 vif 2` `*Jan 1 20:58:34: %7: VRF(0): Ignore No cache message: src 192.168.1.100 for 233.3.3.3 vif 2 in PIM_BOUNDARY_FLT_BOTH range`

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.4.5 Configuring an IP Multicasting Static Route

Configuration Effect

- Configure an IP multicasting static route to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- An IP multicasting static route can be configured on each device unless otherwise specified.

Verification

Run **show ip rpf** { *source-address [group-address]* [**rd** *route-distinguisher*] } [**metric**] to check the RPF information of a specified source.

Related Commands

↘ **Configuring Basic Functions of IP Multicasting**

Command	**ip mroute** *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*]
Parameter Description	*source-address*: Specifies the multicast source address. *mask*: Specifies the mask of the multicast source address. *protocol*: Indicates the unicast routing protocol currently used. *rpf-address*: Specifies the address of the RPF neighbor (next hop of the multicast source). *interface-type interface-number*: Indicates the RPF interface (outgoing interface of the multicast source). *distance*: Specifies the route management distance. The value ranges from 0 to 255. The default value is 0.

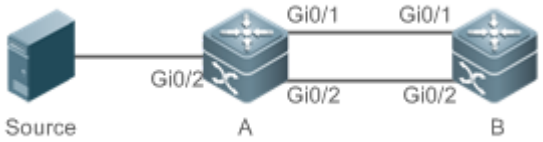
Command Mode	Global configuration mode
Usage Guide	Multicast static routes are applicable only to RPF check. If the IP address of the outgoing interface, but not the next hop, of the static multicast route needs to be specified, the outgoing interface must be a point-to-point type.

Displaying the RFP Information of a Specified Source Address

Command	**show ip rpf** *source-address*
Parameter Description	*source-address*: Specifies the source IP address.
Command Mode	Privilege, global and interface configuration modes
Usage Guide	The three parameters are optional, and the source address and group address must be specified simultaneously. When no source address or group address is specified, all MFC entries are displayed. When only the source address and group address are specified, MFC entries of the source address and group address are displayed.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Supporting PIM-DM

Scenario **Figure 1-7**	
Configuration Steps	● Configure the basic functions of IP multicasting. (Omitted) ● Configure a static route to the receiver on device B.
A	`B# configure terminal` `B(config)# ip mroute 10.10.10.10 255.255.255.255 ospf 192.168.1.1 1`
Verification	Run **show ip rpf** to view the RPF information to the receiver before and after the configuration.

Before Configuration	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 110 Metric: 1
After Configuration	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.10.10/32 RPF type: static RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 1 Metric: 0

Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.

1.4.6 Configuring RPF Route Selection Based on the Longest Match Rule

Configuration Effect

- Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table and select the one with the longest match mask as the RPF route from the three optimal routes.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure RPF route selection based on the longest match rule on each device unless otherwise specified.

Verification

Configure a multicast static route and a unicast static route to have the same priority and configure the unicast static route to have a longer mask length.

- Run **show ip rpf** *source-address* to check the RPF information of a specified source.

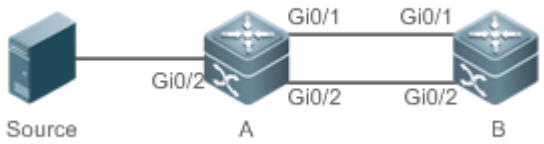
Related Commands

Configuring RPF Route Selection Based on the Longest Match Rule

Command	**ip multicast rpf longest-match**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The steps for selecting RFP routes are as follows: 1. Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table for RPF check. 2. Select one from the three routes as the RPF route. If the longest match rule is used, the route with the longest match mask is selected. If the three routes have the same mask, the one with the highest priority is selected. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route. If the longest match rule is not used, the route with the longest match mask is selected. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

Configuration Example

Creating the IP Multicast Service on the IPv4 Network and Configuring RPF Route Selection Based on the Longest Match Rule

Scenario **Figure 1-8**	
Configuration Steps	● Configure the basic functions of IP multicasting. (Omitted) ● On device B, configure an IP multicast static route whose mask length is smaller than that of the

	unicast static route. ● Configure RPF route selection based on the longest match rule on device B.
B	B# configure terminal B(config)# ip multicast-routing B(config)# ip mroute 10.10.10.10 255.255.0.0 ospf 192.168.1.1 B(config)# ip multicast rpf longest-match
Verification	Run **show ip rpf** to check the RFP information of the multicast source before and after configuring RPF route selection based on the longest match rule.
Before configuration	B#show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.0.0/16 RPF type: static RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 0 Metric: 0
After configuration	B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing prefix-length-preferred lookups across tables Distance: 110 Metric: 1

Common Errors

- An IPv4 unicast route is incorrectly configured.

- IPv4 multicast routing is not enabled on a router.

1.4.7 Configuring Forced Forwarding of Multicast Packets by Software

Configuration Effect

- After configuring this function, all IPv4 multicast data packets destined for the CPU are forcedly forwarded by software.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure forced forwarding of multicast packets by software on each device unless otherwise specified.

Verification

Run **show running-config** to check whether forced forwarding of multicast packets by software is configured.

Related Commands

Configuring Forced Forwarding of Multicast Packets by Software

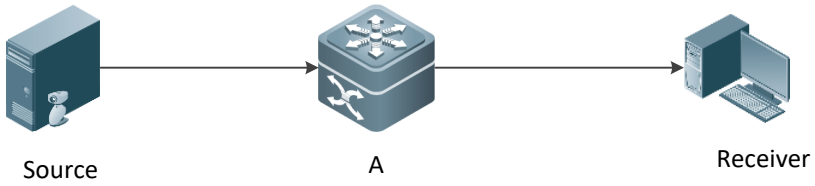
Command	**msf force-forwarding**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Only configuration related to IP multicasting is described.

Creating the IP Multicast Service on the IPv4 Network and Configuring Forced Forwarding of Multicast Packets by Software

Scenario	Basic environment for the IP multicast service

Figure 1-9	
Configuration Steps	● Configure the basic functions of IP multicasting. ● Configure forced forwarding of multicast packets by software.
A	`A# configure terminal` `A(config)#msf force-forwarding`
Verification	Run **show running-config** to check whether forced forwarding of multicast packets by software is configured.
A	`A# show running-config` `…` `msf force-forwarding` `…`

1.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and interrupt services.

Description	Command
Clears the IPv4 multicast forwarding table.	**clear ip mroute** { ***** | *v4group-address* [*v4source-address*] }
Resets statistics in the IPv4 multicast forwarding table.	**clear ip mroute statistics** { ***** | *v4group-address* [*v4source-address*] }

Displaying

Description	Command
Displays the IPv4 multicast forwarding table.	**show ip mroute** [*group-or-source-address* [*group-or-source-address*]] [**dense** | **sparse**] [**summary** | **count**]
Displays IPv4 static multicast route information.	**show ip mroute static**

Description	Command
Displays the RFP Information of a specified IPv4 source address.	**show ip rpf** { *source-address [group-address]* [**rd** *route-distinguisher*] } [**metric**]
Displays information about IPv4 multicast interfaces.	**show ip mvif** [*interface-type interface-number*]
Displays the IPv4 layer-3 multicast forwarding table.	**show ip mrf mfc**
Displays the IPv4 multi-layer multicast forwarding table.	**show msf msc**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs running of the multicast core.	**debug nsm mcast all**
Debugs communication between the IPv4 multicast core and the protocol module.	**debug nsm mcast fib-msg**
Debugs the interface running of the IPv4 multicast core.	**debug nsm mcast vif**
Debugs the interface and entry statistics processing of the IPv4 multicast core.	**debug nsm mcast stats**
Debugs the processing of IPv4 layer-3 multicast packet forwarding.	**debug ip mrf forwarding**
Debugs the operation on layer-3 multicast forwarding entries on an IPv4 network.	**debug ip mrf mfc**
Debugs the processing of layer-3 multicast forwarding events on an IPv4 network.	**debug ip mrf event**
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	**debug msf forwarding**
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	**debug msf mfc**
Debugs the bottom-layer hardware	**debug msf ssp**

Description	Command
processing of IPv4 multi-layer multicast packet forwarding.	
Debugs the invocation of API interfaces provided by IPv4 multi-layer multicast forwarding.	**debug msf api**
Debugs the processing of multi-layer multicast forwarding events on an IPv4 network.	**debug msf event**

2 Configuring IGMP

2.1 Overview

The Internet Group Management Protocol (IGMP) is a member of TCP/IP protocol family. It manages IP multicast members and is used to establish and maintain multicast group membership between hosts and directly neighboring multicast routers. IGMP behaviors are classified into host behaviors and device behaviors.

- At present, three IGMP versions are available, which are IGMPv1, IGMPv2 and IGMPv3.
- All IGMP versions support the Any-Source Multicast (ASM) model.
- IGMPv3 can be directly used for the Source-Specific Multicast (SSM) model.
- IGMPv1 and IGMPv2 can be used for the SSM model only when the IGMP SSM Mapping technology is supported.

Protocols and Standards

- RFC 1112: Host Extensions for IP Multicasting
- RFC 2236: Internet Group Management Protocol, Version 2
- RFC 3376: Internet Group Management Protocol, Version 3
- RFC 4605: Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")

2.2 Applications

Application	Description
Local IGMP Service	Implements the IGMP service in a local network.
IGMP Proxy Service	In a simple tree network topology, use the IGMP proxy service instead of the PIM service.

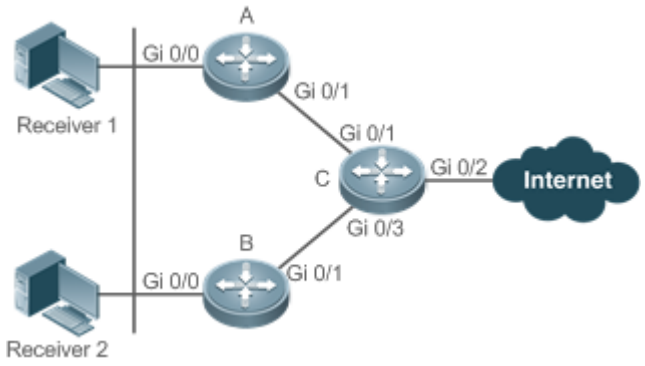
2.2.1 Local IGMP Service

Scenario

As shown in Figure 2-1, receivers 1 and 2 and routers A and B form a local network.

Query packets sent by router A or B are valid in the LAN, whereas Report packets sent by receivers 1 and 2 are also valid locally.

Figure 2-1



Remarks	C is the egress gateway (EG) device. A and B are core routers.

Deployment

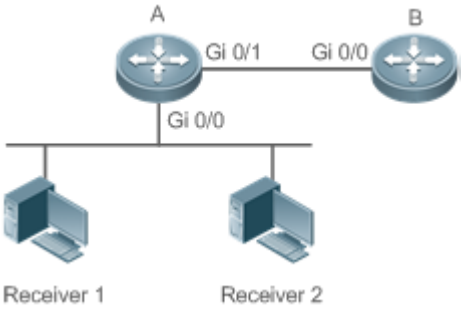
- Routers A, B and C run OSPF.
- The interfaces of A, B and C run multicast protocols (PIM-SM or PIM-DM).

2.2.2 IGMP Proxy Service

Scenario

As shown in Figure 2-2, router A implements the proxy function working as a host and forms a local network group with router B. Router A forwards Report packets sent by receivers 1 and 2.

Figure 2-2



Remarks	Router A implements the proxy function. Router B provides the PIM service.

Deployment

- Routers A and B run OSPF.
- The interfaces of A and B run multicast protocols (PIM-SM or PIM-DM).
- The multicast proxy function is implemented on the interfaces Gi0/0 and Gi0/1 of router A.

2.3 Features

Basic Concepts

Host Behavior and Device Behavior

- Layer-3 multicast devices that run multicast management protocols are called devices and their behaviors are called device behaviors.
- PCs or simulated PCs that run multicast management protocols are called hosts and their behaviors are called host behaviors.

Querier

- Devices compete against each other by comparing IP addresses. Devices with lower IP addresses become queriers and send Query packets regularly.

IGMP Proxy-Service Interface

- This interface performs host behaviors, receives Query packets sent by upstream devices (hence also called uplink interface), and sends Report information collected by the router proxy.

IGMP Mroute–Proxy Interface

- This interface implements the router functions, sends packets received by the IGMP PROXY-SERVICE interface (hence also called downlink interface), and collects host information and sends the host information to the IGMP PROXY-SERVICE interface.

IGMP SSM Mapping

- Mapping of the SSM model. IGMPv1 and IGMPv2 do not support the SSM model, but can enable the SSM-MAP function to support the SSM model.

Overview

Feature	Description
IGMP Router	Sends Query packets and obtains local member information.
IGMP Group Filtering	Filters group members and limit the number of group members.
Static IGMP Group	Static group information is available on a router; therefore, it is unnecessary for the host to send a Report packet to obtain the static group information.
Simulating Hosts to Join IGMP Groups	Simulates the host behavior to directly join a multicast group on an interface.
IGMP Proxy	Use this function in a simple tree network topology where no complex multicast route protocols (such as PIM) need to be executed.

Feature	Description
IGMP SSM Mapping	Provides the SSM model support for IGMPv1 and IGMPv2. When a host joins a group, you can specify a source to save bandwidth and prevent unwanted and invalid multicast data streams from occupying network bandwidth, especially in a network environment where multiple multicast sources share one multicast address.
Router Alert Option	Checks whether IGMP packets contain the Router Alert option and discards the packets without the Router Alert option. Sends IGMP packets with the Router Alert option.

2.3.1 IGMP Router

- This function is used to send Query packets and obtain local member information.

Working Principle

- In a multicast network running the IGMP, a multicast device periodically sends IGMP Query packets and confirms information about local members based on responses.
- Only one multicast device sends IGMP Query packets in one network segment and this device is called querier. The querier is determined by means of selection. Initially, all multicast devices are in the Querier state. When a device receives a membership query from a device with a lower IP address, the device changes from the Querier state to the Non-querier state. Therefore, only one device is in the Querier state finally. This device has the lowest IP address among all multicast devices in the network.
- The querier sends IGMP packets of different versions based on the IGMP version settings. In addition, the following querier parameters can be modified: frequency for the querier to send IGMP Query packets, query times and query interval for the last member, maximum response time of IGMP Query packets, and keepalive time of the existing querier.

Related Configuration

↘ Enabling IGMP

IGMP is disabled on an interface by default.

You can run the **ip pim** { **sparse-mode**| **dense-mode** } command to enable or disable IGMP for an interface.

IGMP can be enabled only when Sparse Mode (SM) or Dense Mode (DM) is configured on the interface.

↘ Specifying the IGMP Version

IGMPv2 is enabled by default.

You can run the **ip igmp version** { **1** | **2** | **3** } command to set or reset the IGMP version.

↘ Configuring the Last-Member Query Interval

The interval for sending the last-member Query packets is 1s by default.

You can run the **ip igmp last-member-query-interval** *interval* command to set or reset the interval for an interface to send Query packets.

A larger value means a larger interval; a smaller value means a smaller interval.

Configuring the Last-Member Query Times

The number of the last-member query times is 2 by default.

You can run the **ip igmp last-member-query-count** *count* command to set or reset the number of the last-member query times.

A larger value means more last-member query times; a smaller value means fewer last-member query times.

Configuring the Common Member Query Interval

The common member query interval is 125s by default.

You can run the **ip igmp query-interval** *seconds* command to set or reset the common member query interval.

A larger value means a larger common query interval; a smaller value means a smaller common query interval.

Configuring the Maximum Response Time

The maximum response time is 10s by default.

You can run the **ip igmp query-max-response-time** *seconds* command to set or reset the maximum response time.

A larger value means longer response time; a smaller value means shorter response time.

Configuring the Querier Timeout

The querier timeout is 255s by default.

You can run the **ip igmp query-timeout** *seconds* command to set the querier timeout.

A larger value means longer survival time; a smaller value means shorter survival time.

2.3.2 IGMP Group Filtering

Filter group members and limit the number of group members.

Working Principle

To prevent hosts in a network segment where an interface resides from joining a multicast group, you can configure an ACL on this interface as a filter. The interface will filter the received IGMP membership Report packets based on this ACL, maintain group membership only for multicast groups allowed by this ACL and set the maximum number of router members.

Related Configuration

Configuring the IGMP Group ACL

By default, no ACL is used and any group is allowed to join.

You can run the **ip igmp access-group** *access-list-name* command to set or reset the multicast group ACL.

After the ACL is configured, a router receives only packets set in the ACL.

↘ Configuring the Maximum Number of IGMP Group Members

The maximum number of IGMP group members is 1,024 by default.

You can run the **ip igmp limit** *number* command to set or reset the maximum number of multicast group members.

A larger value means more members; a smaller value means fewer members.

2.3.3 Static IGMP Group

When static IGMP groups are available on a router, it is unnecessary for the host to send a Report packet to obtain the static group information. The router can directly exchange group information with a PIM router.

Working Principle

You need to set static group information manually.

Related Configuration

↘ Configuring a Static Group

No static group is configured by default.

You can run the **ip igmp static-group** *group-address* command to configure a static group.

2.3.4 Simulating Hosts to Join IGMP Groups

Simulate the host behavior to directly join a multicast group on an interface.

Related Configuration

↘ Configuring the Join-Group function

No join-group information is set by default.

You can run the **ip igmp join-group** *group-address* command to configure the address of the multicast group to be joined by the simulated host.

2.3.5 IGMP Proxy

Use this function in a simple tree network topology where no complex multicast route protocols (such as PIM) need to be executed. In this way, a downstream proxy host can send IGMP packets and maintain the membership.

Working Principle

When an upstream router is configured as an IGMP proxy-service interface, it is equal to a host that can receive Query packets sent by upstream routers or forward group information sent by downstream hosts. When a downstream router is configured as an IGMP multicast proxy interface, it is equal to a router that can forward Query packets sent by upstream routers or receive Report packets sent by downstream routers.

Related Configuration

Configuring the IGMP Proxy Service

The IGMP proxy service function is disabled by default.

You can run the **ip igmp proxy-service** command to enable the IGMP proxy service.

This function is mandatory when a proxy is to be used.

Configuring the IGMP Mroute Proxy

The IGMP mroute proxy function is disabled by default.

You can run the **ip igmp mroute-proxy** *interfacename* command to enable the IGMP mroute proxy.

This function is mandatory when a proxy is to be used.

2.3.6 IGMP SSM Mapping

Provide the SSM model support for IGMPv1 and IGMPv2. When a host joins a group, you can specify a source to save bandwidth and prevent unwanted and invalid multicast data streams from occupying network bandwidth, especially in a network environment where multiple multicast sources share one multicast address.

Working Principle

Based on IGMP v1/v2, IGMPv3 provides an extra function, namely, the multicast source filter function. In IGMPv1/v2, a host determines to join a group only based on the group address and then receive multicast streams sent to this group address from any source. A host using IGMPv3 advertises the multicast group that the host wants to join and the addresses of multicast sources from which this host wants to receive packets. IGMPv1 and IGMPv2 also implement "source address filtering" in some sense; however, they implement this function on the multicast receivers by enabling the SSM mapping function and configuring the static SSM mapping group.

Related Configuration

Enabling IGMP SSM Mapping

The SSM mapping function is disabled by default.

You can run the **ip igmp ssm-map enable** command to enable the function.

Mandatory.

Configuring Static IGMP SSM Mapping

No static SSM mapping is set by default.

You can run the **ip igmp ssm-map static** *access-list-num A.B.C.D* command to configure static SSM mapping.

2.3.7 Router Alert Option

Check whether IGMP packets contain the Router Alert option and discard packets without the Router Alert option.

Support sending IGMP packets containing the Router Alert option.

Working Principle

If a packet contains the Router Alert option, the device needs to check the packet in depth and updates the control data accordingly. If the packet does not contain the option, the device does not check the packet.

After Router Alert option check is enabled, the IGMP packets not containing the Router Alert option are discarded.

After enabled with the function of sending packets with Router Alert option, the device sends IGMP packets with Router Alert option encapsulated.

Related Configuration

Checking Router Alert Option

Router Alert option check is disabled by default.

You can run the **ip igmp enforce-router-alert** command to enable the function.

Sending IGMP Packets with Router Alert Option Encapsulated

Packets are sent without the Router Alert option by default.

You can run the **ip igmp send-router-alert** command to enable the function.

2.4 Configuration

Configuration	Description and Command	
Configuring IGMP Basic Functions	(Mandatory) It is used to set up the multicast service.	
	ip multicast-routing	Enables the IPv4 multicast routing function.
	ip pim { **sparse-mode**| **dense-mode** }	Enables the PIM-SM or PIM-DM function.
Configuring IGMP Routers	**ip igmp version** { **1** | **2** | **3** }	Specifies the IGMP version.
	ip igmp last-member-query-interval *interval*	Configures the last-member query interval.
	ip igmp last-member-query-count *count*	Configures the last-member query times.
	ip igmp query-interval *seconds*	Configures the membership query interval.
	ip igmp query-max-response-time *seconds*	Configures the maximum response time.
	ip igmp query-timeout *seconds*	Configures the querier timeout.
Configuring IGMP Group Filtering	**ip igmp access-group** *access-list*	Configures the IGMP group ACL.
	ip igmp limit *number* [**except** *access-list*]	Configures the maximum number of IGMP group members.

Configuring IGMP Proxy	**ip igmp proxy-service**	Configures the IGMP proxy service.
	ip igmp mroute-proxy *interface-type interface-number*	Configures the IGMP mroute proxy.
Configuring IGMP SSM Mapping	**ip igmp ssm-map enable**	Enables IGMP SSM mapping.
	ip igmp ssm-map static *access-list source-address*	Configures static IGMP SSM mapping.
Configuring Alert Option	**ip igmp enforce-router-alert**	Checks the Router Alert option.
	ip igmp send-router-alert	Sends IGMP packets containg the Router Alert option.

2.4.1 Configuring IGMP Basic Functions

Configuration Effect

- Enable the multicast routing function of a local network and collect group information of the local network.

Notes

- An interface must be enabled with the PIM-SM or PIM-DM function.

Configuration Steps

Enabling the IPv4 Multicast Routing Function

- Mandatory.
- If there is no special requirement, the IPv4 multicast routing function should be enabled on each router in the local network.

Enabling the PIM-SM or PIM-DM Function

- Mandatory.
- If there is no special requirement, the PIM-SM or PIM-DM function should be directly enabled on an interface of the local network.

Verification

Run the **show ip igmp interface** *interface-type interface-number* command to check whether IGMP is enabled on the interface.

Related Commands

Enabling the IPv4 Multicast Routing Function

Command	**ip multicast-routing**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling the PIM-SM or PIM-DM Function

Command	**ip pim** { **sparse-mode** | **dense-mode** }
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be layer-3 interfaces, including routing interfaces, L3AP, SVI and loopback interfaces. All PIM interfaces should be accessible to IPv4 unicast routes.

Configuration Example

Enabling IGMP for a Local Network

Scenario	● Configure an IPv4 unicast routing protocol (such as OSPF) on a router and ensure that the loopback interface is accessible to a unicast route. ● Enable the IPv4 multicast route function on all routers. ● Enable the PIM-SM or PIM-DM function on interfaces interconnecting devices and interfaces connecting user hosts and multicast sources.
	`VSU(config)#ip multicast-routing` `VSU(config)#int gi 0/5` `VSU(config-if-GigabitEthernet 0/5)#ip add 192.168.1.90 255.255.255.0` `VSU(config-if-GigabitEthernet 0/5)#ip pim sparse-mode`
Verification	Run the **show ip igmp interface** *interface-type interface-number* command to check whether IGMP is enabled on the interface.
	`VSU#show ip igmp interface gigabitEthernet 0/5` `Interface GigabitEthernet 0/5 (Index 5)` `IGMP Active, Querier, Version 2 (default)` `Internet address is 192.168.1.90` `IGMP interface limit is 1024` `IGMP interface has 1 group-record states` `IGMP interface has 0 static-group records`

	IGMP activity: 3 joins, 0 leaves IGMP query interval is 125 seconds IGMP querier timeout is 255 seconds IGMP max query response time is 10 seconds Last member query response interval is 10 Last member query count is 2 Group Membership interval is 260 seconds Robustness Variable is 2

Common Errors

- Routers in the network are not enabled with the multicast routing function.
- No multicast interface is available in the network.

2.4.2 Configuring IGMP Routers

Configuration Effect

- Modify the querier timeout and IGMP router parameters will affect the type of packets to be sent and the sending method.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

Specifying the IGMP Version

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Configuring the Last-Member Query Interval

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Configuring the Last-Member Query Times

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Configuring the Common Member Query Interval

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Configuring the Maximum Response Time

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Verification

Run the **show ip igmp interface** *interface-type interface-number* command to display the interface configurations.

Related Commands

Specifying the IGMP Version

Command	**ip igmp version** { **1** | **2** | **3** }
Parameter Description	1: Indicates IGMPv 1. 2: Indicates IGMPv 2. 3: Indicates IGMPv 3.
Command Mode	Interface configuration mode
Usage Guide	After this command is configured, IGMP will automatically restart.

Configuring the Last-Member Query Interval

Command	**ip igmp last-member-query-interval** *interval*
Parameter Description	*Interval*: Indicates the interval for sending the Query packets of a specific group. The value ranges from 1 to 255 in the unit of 0.1s, and the default value is 10 (namely, 1s).
Command Mode	Interface configuration mode
Usage Guide	This command applies only to IGMPv2 or IGMPv3. When an interface receives a Leave packet, the interface sends Query packets of the group continually and waits for a response from the host. After timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the interface from the IGMP group. The timeout duration is equal to the value of **last-member-query-interval** multiplied by **last-member-query-count** plus 1/2 of **query-max-response-time**.

Configuring the Last-Member Query Times

Command	**ip igmp last-member-query-count** *count*
Parameter Description	*count*: Indicates the times for sending the Query packets of a specific group, ranging from 2 to 7. The default value is 2.
Command Mode	Interface configuration mode
Usage Guide	This command applies only to IGMPv2 or IGMPv3. When an interface receives a Leave packet, the interface sends Query packets of the group continually and waits for a response from the host. After timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the interface from the IGMP group. The timeout duration is equal to the value of **last-member-query-interval** multiplied by **last-member-query-count** plus 1/2 of **query-max-response-time**.

Configuring the Common Member Query Interval

Command	**ip igmp query-interval** *seconds*
Parameter Description	*seconds*: Indicates the common member query interval, ranging from 1 to 18,000s. The default value is 125.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Maximum Response Time

Command	**ip igmp query-max-response-time** *seconds*
Parameter Description	*seconds*: Indicates the maximum response time, ranging from 1 to 25s. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	After sending Query packets, the interface waits for a response. If timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the group information.

Configuring the Querier Timeout

Command	**ip igmp query-timeout** *seconds*
Parameter Description	*seconds*: Indicates the keepalive time of the querier, ranging from 60s to 300s. The default value is 255s.
Command Mode	Interface configuration mode
Usage Guide	After sending Query packets, an interface waits for Query packets sent by other devices. If timeout occurs,

	the IGMP router assumes that the querier is unique in the directly connected network segment.

Configuration Example

Configuring Basic Router Parameters

Scenario	● Configure basic functions of IGMP. ● Specify the IGMPv3. ● Configure the last-member query interval to 15 (1.5s). ● Configure the number of the last-member queries to 3. ● Configure the common member query interval to 130s. ● Configure the maximum response time to 15s. ● Configure the querier timeout to 280s.
	VSU(config-if-GigabitEthernet 0/5)#ip igmp version 3 VSU(config-if-GigabitEthernet 0/5)#ip igmp last-member-query-count 3 VSU(config-if-GigabitEthernet 0/5)#ip igmp last-member-query-interval 15 VSU(config-if-GigabitEthernet 0/5)#ip igmp query-interval 130 VSU(config-if-GigabitEthernet 0/5)#ip igmp query-max-response-time 15 VSU(config-if-GigabitEthernet 0/5)#ip igmp query-timeout 280
Verification	Run the **show ip igmp interface** *interface-type interface-number* command to check the IGMP functions of the interface.

	VSU#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Enabled, Active, Querier, Version 3 Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group-record states IGMP interface has 0 static-group records IGMP activity: 3 joins, 0 leaves IGMP query interval is 130 seconds IGMP querier timeout is 280 seconds IGMP max query response time is 15 seconds Last member query response interval is 15 Last member query count is 3 Group Membership interval is 275 seconds Robustness Variable is 2 VSU#

Common Errors

- The basic functions of IGMP are not enabled.

2.4.3 Configuring IGMP Group Filtering

Configuration Effect

- A router filters IGMP group members.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

↘ Configuring the IGMP Group ACL

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

↘ Configuring the Maximum Number of IGMP Group Members

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Verification

IGMP Group ACL

- Configure an interface to allow only groups in ACL 1 to join. The access addresses of ACL 1 are 225.0.0.1~225.0.0.255.
- Configure the interface to join a group whose address is 225.0.0.5.
- Configure the interface to join a group whose address is 236.0.0.5.
- View the group information of the current interface.

Maximum Number of IGMP Group Members

- Set the maximum member quantity to 5 on an interface.
- Configure the interface to join a group whose address is from 225.0.0.5 to 225.0.0.10.
- View the group information of the interface.

Related Commands

Configuring the IGMP Group ACL

Command	**ip igmp access-group** *access-list*
Parameter Description	*access-list*: Defines a group address range by using a standard IP ACL or an extended ACL. The value ranges from 1 to 199, 1300 to 2699 and characters.
Command Mode	Interface configuration mode
Usage Guide	Configure this command on an interface to control the groups that hosts in a directly connected network segment can join. Use an ACL to limit the group address range. If Report packets denied by the ACL are received, the packets will be discarded. When IGMPv3 is enabled, this command supports an extended ACL. If the received IGMP Report information is (S1,S2,S3…Sn,G), this command will apply the corresponding ACL to the (0,G) information for matching. Therefore, you must configure a (0,G) record explicitly for the extended ACL in order to normally filter (S1,S2,S3…Sn,G).

Configuring the Maximum Number of IGMP Group Members

Command	**ip igmp limit** *number* [**except** *access-list*]
Parameter Description	**vrf** *vrf-name*: Specifies a VRF. This parameter applies only to the global configuration mode. number: Indicates the maximum number of IGMP group members, whose value range varies with devices. The default value is 1,024 for an interface and 65,536 globally.

	except *access-list*: Indicates that the groups in the ACL are not counted. **access-list** indicates a standard IP ACL. The value ranges from 1 to 99, 1300 to 1999 and words.
Command Mode	Interface configuration mode
Usage Guide	Global configuration mode: Limits the maximum quantity of the IGMP group members in a system. Interface configuration mode: limits the maximum quantity of IGMP group members on an interface. If the quantity of group members exceeds the interface or global limit, the Report packets received subsequently will be ignored. If an Except ACL is configured, Report packets within a specified range can be normally processed; therefore, the generated group members are not counted. The interface and global configurations can be performed independently. If the global quantity limit is smaller than that for an interface, the global configuration shall be used.

Configuration Example

Configuring IGMP Group Filtering

Scenario	● Configure the basic functions of IGMP. ● Configure the access address range of ACL 1 from 225.0.0.1 to 225.0.0.255. ● Set the address of the group to be joined to 225.0.0.5. ● Set the address of the group to be joined to 236.0.0.5.
	`VSU(config)#access-list 1 permit 225.0.0.1 225.0.0.255` `VSU(config-if-GigabitEthernet 0/5)#ip igmp access-group 1` `VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.5` `VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 236.0.0.5`
Verification	Run the **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**] command to display the group information of the interface.
	`VSU(config-if-GigabitEthernet 0/5)#show ip igmp groups` `IGMP Connected Group Membership` `Group Address  Interface  Uptime  Expires  Last Reporter` `225.0.0.5  GigabitEthernet 0/5  00:14:00  00:02:45  192.168.1.90`

Configuring the Maximum Number of IGMP Group Members

Scenario	● Configure the basic functions of IGMP. ● Configure the maximum number of IGMP group members for the interface to 5. ● Add group information (225.0.0.5~225.0.0.12). ● View group information.

	VSU(config-if-GigabitEthernet 0/5)#ip igmp limit 5 VSU(config-if-GigabitEthernet 0/5)# VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.5 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.6 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.7 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.8 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.9 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.10 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.11 VSU(config-if-GigabitEthernet 0/5)#ip igmp join-group 225.0.0.12
Verification	Run the **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**] command to display the group information of the interface.
	VSU(config-if-GigabitEthernet 0/5)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 225.0.0.5 GigabitEthernet 0/5 00:20:15 00:03:09 192.168.1.90 225.0.0.6 GigabitEthernet 0/5 00:20:24 00:02:58 192.168.1.90 225.0.0.7 GigabitEthernet 0/5 00:00:15 00:04:29 192.168.1.90 225.0.0.8 GigabitEthernet 0/5 00:00:13 00:04:34 192.168.1.90 225.0.0.9 GigabitEthernet 0/5 00:00:11 00:04:33 192.168.1.90

Common Errors

- The basic functions of IGMP are not enabled.

2.4.4 Configuring IGMP Proxy

Configuration Effect

- Configure the router proxy function and collect local member information.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

↘ **Configuring the IGMP Proxy Service**

- Optional.
- If there is no special requirement, you can perform this configuration on directly connected upstream router interfaces.

Configuring the IGMP Mroute Proxy

- Optional.
- If there is no special requirement, you can perform this configuration on directly connected downstream host interfaces.

Verification

- Set interface 7 for directly connecting to an upstream router as a multicast proxy server.
- Set interface 1 for directly connecting to a downstream host as a multicast proxy.
- Set interface 1 to be joined by groups whose addresses are 225.0.0.6 and 225.5.5.5.
- View the current group information.

Related Commands

Configuring the IGMP Proxy Service

Command	**ip igmp proxy-service**
Parameter Description	*N/A*
Command Mode	Interface configuration mode
Usage Guide	Run the **ip igmp proxy-service** command to set the uplink interface as a Proxy-Service interface. Run the **ip igmp mroute-proxy** command to set the downlink interface as a Mroute-Proxy interface. Forward IGMP Query packets from the Proxy-Service interface to the Mroute-Proxy interface. Forward IGMP Report packets from the Mroute-Proxy interface to the Proxy-Service interface. A device allows a maximum of 32 Proxy-Service interfaces. After a Proxy-Service interface receives an IGMP Query packet, the interface sends a response based on the IGMP group member records. If the **switchport** command is executed on the Proxy-Service interface, the **ip igmp mroute-proxy** command configured on the Mroute-Proxy interface will be deleted automatically.

Configuring the IGMP Mroute Proxy

Command	**ip igmp mroute-proxy** *interface-type interface-number*
Parameter Description	*N/A*
Command Mode	Interface configuration mode
Usage Guide	Run the **ip igmp proxy-service** command to set the uplink interface as a Proxy-Service interface. Run the **ip igmp mroute-proxy** command to set the downlink interface as a Mroute-Proxy interface. Forward IGMP Query packets from the Proxy-Service interface to the Mroute-Proxy interface. Forward

	IGMP Report packets from the Mroute-Proxy interface to the Proxy-Service interface.

Configuration Example

Scenario	● Configure basic functions of IGMP. ● Configure interface 7 as a proxy server. ● Configure interface 1 as a multicast proxy. ● Set interface 1 to be joined by groups whose addresses are 225.0.0.6 and 225.5.5.5.
	VSU(config-if-GigabitEthernet 0/7)#ip igmp proxy-service VSU(config-if-GigabitEthernet 0/7)#exit VSU(config)#int gi 0/1 VSU(config-if-GigabitEthernet 0/1)#ip igmp mroute-proxy gigabitEthernet 0/7 VSU(config-if-GigabitEthernet 0/1)#ip igmp join-group 225.0.0.6 VSU(config-if-GigabitEthernet 0/1)#ip igmp join-group 225.5.5.5
Verification	Run the **show ip igmp groups** [*interface-type interface-number*] [*group-address*] [**detail**] command to display the group information of the interface.
	VSU(config-if-GigabitEthernet 0/1)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 225.0.0.6 GigabitEthernet 0/1 00:23:05 00:02:40 192.168.36.90 225.5.5.5 GigabitEthernet 0/1 00:22:06 00:02:41 192.168.36.90 IGMP Proxy-server Connected Group Membership Group Address Interface Uptime 225.0.0.6 GigabitEthernet 0/7 00:23:05 225.5.5.5 GigabitEthernet 0/7 00:22:06 VSU(config-if-GigabitEthernet 0/1)#

Common Errors

- The basic functions of IGMP are not enabled.

2.4.5 Configuring IGMP SSM Mapping

Configuration Effect

- IGMPv3 supports source filtering; however, IGMPv1 and IGMPv2 do not support source filtering, but provides the SSM mapping function to filter sources.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

Enabling SSM Mapping

(Mandatory) Enable the SSM mapping function.

Enable the SSM mapping function on a router.

Configuring Static SSM Mapping

Optional.

Configure this function on routers enabled with SSM mapping.

Verification

Run the **show ip igmp ssm-mapping** [*group-address*] command to display SSM mapping information.

Related Commands

Enabling SSM Mapping

Command	**ip igmp ssm-map enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **ip igmp ssm-map enable** command to enable the SSM mapping function. Run the **ip igmp ssm-map static** command to set static mapping entries. Run IGMPv3 on the interface. When IGMPv1 or IGMPv2 Report packets are received, source addresses of static mappings can be added.

Configuring Static SSM Mapping

Command	**ip igmp ssm-map static** *access-list source-address*
Parameter Description	*access-list*: Indicates the group address range set by a standard IP ACL. The value ranges from 1 to 99, 1300 to 1999 and words.

	source-address: Indicates the source address.
Command Mode	Global configuration mode
Usage Guide	Run the **ip igmp ssm-map enable** command to enable the SSM mapping function. Run the **ip igmp ssm-map static** command to set static mapping entries. Run IGMPv3 on the interface. When IGMPv1 or IGMPv2 Report packets are received, source addresses of static mappings can be added.

Configuration Example

Scenario	● Configure the basic functions of IGMP. ● Enable SSM mapping. ● Configure static SSM mapping ACL 1.
	`VSU(config)#ip igmp ssm-map enable` `VSU(config)#ip igmp ssm-map static 1 192.168.5.9`
Verification	Run the **show ip igmp ssm-mapping** [**group-address**] command to display SSM mapping information.
	`VSU#show ip igmp ssm-mapping` `SSM Mapping : Enabled` `Database : Static mappings configured`

Common Errors

- The basic functions of IGMP are not enabled.

2.4.6 Configuring Alert Option

Configuration Effect

- Check whether IGMP packets contain the Router Alert option and discards the packets without the Router Alert option.
- Support sending IGMP packets with the Router Alert option.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

↘ Checking Router Alert Option

Optional.

↘ Sending IGMP Packets with Router Alert Option Encapsulated

Optional,

Verification

Checking Router Alert Option

Check whether the IGMP-enabled interface discards the IGMP packets without the Router Alert option.

Sending IGMP Packets with Router Alert Option Encapsulated

Check whether the IGMP-enabled interface sends the IGMP packets containing the Router Alert option.

Related Commands

Checking Router Alert Option

Command	**ip igmp enforce-router-alert**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **ip igmp enforce-router-alert** command to enable Router Alert option check. Run the **no ip igmp enforce-router-alert** command to disable Router Alert option check.

Sending IGMP Packets with Router Alert Option Encapsulated

Command	**ip igmp send-router-alert**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run the **ip igmp send-router-alert** command to enable the function of sending IGMP packets containing Router Alert option. Run the **no ip igmp send-router-alert** command to disable the function.

Configuration Example

Checking Router Alert Option

Scenario	● Configure the basic functions of IGMP. ● Configure Router Alert option check.
	`VSU(config)#ip igmp enforce-router-alert`

Verification	IGMP packets containing Router Alert option 225.1.1.1 are sent to the IGMP-enabled interface and these packets are processed. Run the **show ip igmp groups** command and you will see 225.1.1.1. IGMP packets not containing Router Alert option 225.1.1.1 are sent to the IGMP-enabled interface and these packets are discarded. Run the **show ip igmp groups** command and you will not see 225.1.1.1

Sending IGMP Packets with Router Alert Option Encapsulated

Scenario	● Configure the basic functions of IGMP. ● Configure the function of sending IGMP packets containing router alert option.
	`VSU(config)#ip igmp send-router-alert`
Verification	Check whether the IGMP-enabled interface sends the IGMP packets containing the Router Alert option.

2.5 Monitoring

Clearing

Description	Command
Clears dynamic group membership from the IGMP buffer.	**clear ip igmp group**
Clears interface information from the IGMP buffer.	**clear ip igmp interface** *interface-type interface-number*

Displaying

Description	Command
Displays all groups in a directly connected subnet.	**show ip igmp groups**
Displays details about all groups in a directly connected subnet.	**show ip igmp groups detail**
Displays specified groups in a directly connected subnet.	**show ip igmp groups** *A.B.C.D*
Displays details about specified groups in a directly connected subnet.	**show ip igmp groups** *A.B.C.D* **detail**
Displays IGMP configurations of a specified interface in a directly connected subnet.	**show ip igmp interface** *interface-type interface-number*

Displays details about all groups of a specified interface in a directly connected subnet.	**show ip igmp groups** *interface-type interface-number* **detail**
Displays information about a specified group of a specified interface in a directly connected subnet.	**show ip igmp groups** *interface-type interface-number A.B.C.D*
Displays details about a specified group of a specified interface in a directly connected subnet.	**show ip igmp groups** *interface-type interface-number A.B.C.D* **detail**
Displays configurations of an IGMP interface.	**show ip igmp interface** [*interface-type interface-number*]
Displays configurations of all IGMP interfaces.	**show ip igmp interface**
Displays configurations of IGMP SSM mapping.	**show ip igmp ssm-mapping**
Displays the information of IGMP SSM mapping to *A.B.C.D.*	**show ip igmp ssm-mapping** *A.B.C.D*

Debugging

Description	Command
Displays whether IGMP debugging is enabled.	**show debugging**
Debugs all IGMP information.	**debug ip igmp all**
Debugs IGMP packet decoding.	**debug ip igmp decode**
Debugs IGMP packet encoding.	**debug ip igmp encode**
Debugs IGMP events.	**debug ip igmp events**
Debugs IGMP FSM.	**debug ip igmp fsm**
Debugs IGMP state machine.	**debug ip igmp tib**
Debugs IGMP warning.	**debug ip igmp warning**

3 Configuring PIM-DM

3.1 Overview

Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol.

A multicast source sends a packet to a group address. The packet is forwarded by network devices hop by hop and finally reaches the group members. On layer-3 network devices, PIM is used to create and maintain multicast routing entries, so as to support multicast forwarding.

PIM works in two modes: Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM is applicable to large-scale networks where group members are sparsely distributed in a wide scope.
- PIM-DM is applicable to small networks where group members are densely distributed.

Protocols and Standards

- RFC3973: Protocol Independent Multicast - Dense Mode (PIM-DM)
- RFC2715: Interoperability Rules for Multicast Routing Protocols

3.2 Applications

Application	Description
Providing the Multicast Service in the Same Network	The multicast service is provided in the same network.
PIM-DM Application in a Hot Backup Environment	The multicast PIM-DM protocol runs in a hot backup environment.

3.2.1 Providing the Multicast Service in the Same Network

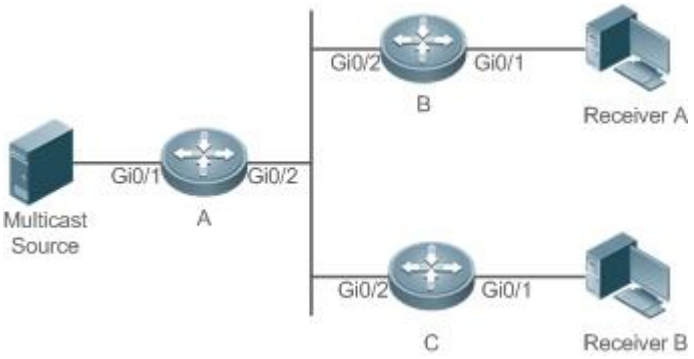
Scenario

The multicast service is provided in the same network.

The following figure is taken as an example:

- A multicast source sends a multicast packet, and Receiver A and Receiver B in the same network receive the multicast packet.

Figure 3-1



Remarks	A, B, and C are Layer-3 routers. The multicast source is connected to the Gi0/1 interface of A, Receiver A is connected to the Gi0/1 interface of B, and Receiver B is connected to Gi0/1 of C.

Deployment

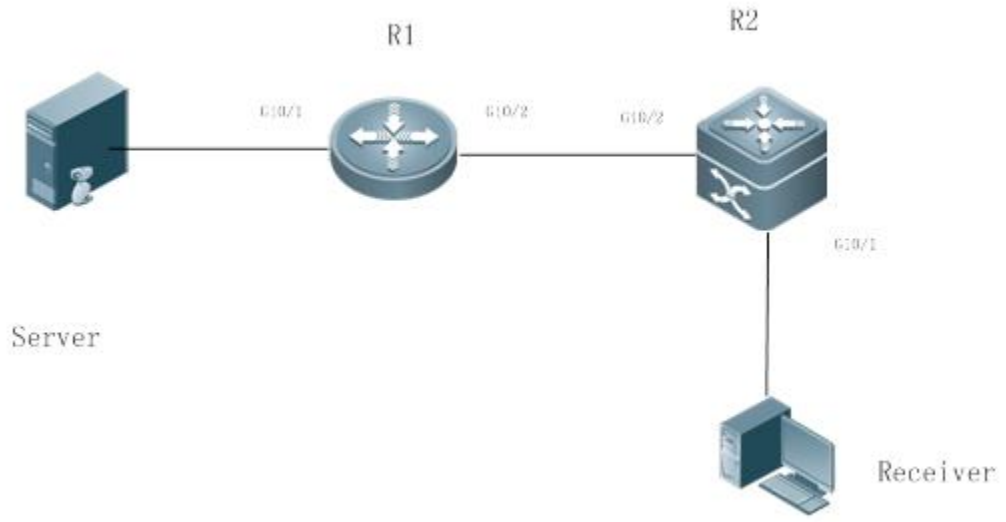
- Run the Open Shortest Path First (OSPF) protocol in the same network to implement unicast routing.
- Run the PIM-DM protocol in the same network to implement multicast routing.
- Run the Internet Group Management Protocol (IGMP) in a user host network segment to implement group member management.

3.2.2 PIM-DM Application in a Hot Backup Environment

Scenario

In a hot backup environment, run PIM-DM. A device performs hot backup switching to ensure that traffic is not interrupted.

Figure 3-2



Remarks	R1 is connected to the video server, R2 is directly connected to the receiver, and R2 runs in hot backup mode. A Layer-3 multicast protocol runs on R1 and R2.

Deployment

- Run OSPF on R1 and R2 to implement unicast routing.
- Run PIM-DM on R1 and R2 to implement multicast routing.
- Make R2 run in a hot backup environment.

Remarks	R2 may perform hot backup switching in the hot backup environment. In this case, the query interval of PIM Hello packets (the default value is 30 seconds) needs to be adjusted on R2 because the keepalive timer of the neighbor in PIM Hello packets of R1 may have expired (the default value is 3.5 times the query interval, that is, 105 seconds). The multicast function relies on the unicast function currently, and the multicast function starts convergence after the unicast function convergence is complete. For example, the default graceful restart (GR) convergence time of the unicast function is 120 seconds. It is recommended that the query interval of PIM Hello packets be set to 60 seconds. The keepalive time of the neighbor in PIM Hello packets is 210 seconds. In this scenario, the query interval of PIM Hello packets need to be set with a reference to the GR convergence time of the unicast function and the value of 3.5 times the query interval of PIM Hello packets must be larger than the GR convergence time of the unicast function. In a hot backup environment, it is recommended that the query interval of PIM Hello packets be larger than the default value (30 seconds). Otherwise, the keepalive timer of the neighbor in PIM Hello packets of the peer end times out during hot backup switching.

3.3 Features

Basic Concepts

PIM Router and PIM Interface

Routers where the PIM protocol is enabled are called PIM Routers. Interfaces where the PIM protocol is enabled are called PIM interfaces.

Multicast packets are forwarded on PIM routers. The PIM interfaces where multicast packets are received are called Upstream Interfaces, and the PIM interfaces where multicast packets are sent are called Downstream Interfaces.

The network segments where upstream interfaces are located are called Upstream Network Segments. The network segments where downstream interfaces are located are called Downstream Network Segments.

PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On some PIM interfaces, borders can be set to divide a large PIM network into multiple PIM domains. The borders are able to reject specified multicast packets or limit the transmission of PIM messages.

Multicast Distribution Tree

Multicast packets are packets transmitted from one point to multiple points. The forwarding path is in a tree structure. This forwarding path is called the Multicast Distribution Tree (MDT).

(*,G), (S,G)

- (*,G): Packets sent from any source to Group G, the corresponding routing entries, and the forwarding path called Rendezvous Point Tree (RPT).
- (S,G): Packets sent from Source S to Group G, the corresponding routing entries, and the forwarding path called Shortest Path Tree (SPT).

Overview

Feature	Description
PIM-DM Neighbor	Neighbor relationships are established between PIM routers to form a PIM network.
PIM-DM MDT	PIM-DM creates the MDT by using flooding, pruning, and grafting.
PIM-DM SRM	PIM-DM uses a State Refresh Message (SRM) to update the network state.
MIB	The Simple Network Management Protocol (SNMP) manager uses information in the Management Information Base (MIB) to directly manage the PIM-DM function.

3.3.1 PIM-DM Neighbor

Neighbor relationships are established between PIM routers to form a PIM network. Neighbor relationships must be established between PIM routers before PIM control messages can be exchanged or multicast packets can be forwarded.

Working Principle

A Hello message is sent from a PIM interface. For the IPv4 multicast packet with the Hello message encapsulated, the destination address is 224.0.0.13 (indicating all PIM routers in the same network segment), the source address is the IP address of the PIM interface, and the Time To Live (TTL) value is 1. For the IPv6 multicast packet with the Hello message encapsulated, the destination address is ff02::d.

Function of a Hello message: It is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.

Discovering Neighbors

PIM routers in the same network segment receive multicast packets from the destination address 224.0.0.13 or ff02::d. In this way, the PIM routers obtain neighbor information and establish neighbor relationships.

When a PIM interface is enabled or detects a new neighbor, a Triggered-Hello-Delay message is used to generate a random time. Within the time, the interface sends Hello packets.

Coordinating Protocol Parameters

A Hello message includes multiple protocol parameters, which are described as follows:

– DR_Priority: Router interfaces contend for the designated router (DR) based on their DR priorities. A higher priority means a higher chance of winning.

– Holdtime: Time in which a neighbor is held in the reachable state

– LAN_Delay: LAN delay for transmitting a Prune message in a shared network segment

– Override-Interval: Prune override time carried in a Hello message.

When a PIM router receives a Prune message from an upstream interface, it indicates that downstream interfaces exist in the shared network segment. If the PIM router still needs to receive multicast data, the PIM router must sent a Prune Override message to the upstream interface within the Override-Interval.

LAN_Delay + Override-Interval = PPT (Prune-Pending Timer). After a PIM router receives a Prune message from an downstream interface, the PIM router will not immediately perform pruning until PPT times out. Within the time of PPT, if the PIM router receives a Prune rejection message from the downstream interface, the PIM router cancels pruning.

Maintaining Neighbor Relationships

A Hello message is sent periodically between PIM routers. If a Hello packet is not received from a PIM neighbor within Holdtime, the neighbor is considered unreachable and is deleted from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an upstream or downstream neighbor in an MDT is unreachable, multicast routes converge again and the MDT is reshaped.

Related Configuration

Enabling PIM-DM on an Interface

By default, PIM-DM is disabled on an interface.

Use the **ip pim dense-mode** command to enable or disable PIM-DM on an interface.

PIM-DM must be enabled on an interface to involve the interface in the PIM protocol.

Setting the Interval of Hello Messages on an Interface

By default, a Hello message is sent at an interval of 30 seconds.

The **ip pim query-interval** *interval-seconds* command is used to adjust the interval of Hello messages. The value of the interval ranges from 1 to 65,535.

A Hello message is transmitted less frequently when the value of *interval-seconds* is larger.

3.3.2 PIM-DM MDT

The three basic mechanisms dense-mode PIM uses to build multicast forwarding trees are: flood, prune, and graft.

Working Principle

When a multicast source sends multicast packets, the system forwards them to the outgoing interfaces of multicast neighbors and local members. The Reverse Path Forwarding (RPF) check needs to be conducted on all packets received through the upstream interface of the device. Packets that fail the RPF check will be discarded. Multicast packets that pass the RPF check are further forwarded if there is an outgoing interface. If no outgoing interface is available, the device sends a prune packet to the upstream interface. After receiving the prune packet, the upstream interface identifies the source interface of the prune packet as the Pruned state and sets the Pruned Timer (PI). In this way, a multicast forwarding tree with the multicast source as the root is created.

When the system receives a Join message from a local member, if a downstream device in the Pruned state sends a Graft message to the upstream device, the upstream device returns a Graft-Ack message and resumes forwarding of multicast data to the interface of the downstream device after receiving the Graft message.

In environment deployment, when multiple PIM-DM neighbors are created through multiple links between devices and downstream devices need to receive no or few packets, the CPU usage may be high. In this scenario, PIM-SM is recommended for the environment deployment

Related Configuration

Configuring the Prune Override Interval on an Interface

By default, the prune override interval is 500 ms.

Run the **ip pim override-interval** *interval-milliseconds* command to change the prune override interval.

3.3.3 PIM-DM SRM

PIM-DM uses an SRM to refresh the network state.

Working Principle

Devices connected to a multicast source periodically send SRMs to downstream devices to notify changes of the network topology. After receiving the SRMs, the adjacent devices receiving the SRMs add the local topology state information to the messages by modifying some fields in SRMs, and send the messages to downstream devices. When the messages reach leaf devices, the state information of the entire network is updated.

Related Configuration

Disabling the Processing and Forwarding of SRMs

By default, the processing and forwarding of SRMs are enabled.

The **ip pim state-refresh disable** command is used to disable the processing and forwarding of SRMs.

Disabling the SRM function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, it is recommended not to disable SRM in general conditions.

Setting the Interval of SRMs

By default, an SRM is sent at an interval of 60 seconds.

The **ip pim state-refresh origination-interval** *interval-seconds* command is used to adjust the interval of SRMs. The value of the interval ranges from 1 to 100.

SRMs are transmitted less frequently when the value of *interval-seconds* is larger.

Only devices that are directly connected to a multicast source will periodically send a PIM SRM to downstream interfaces. For a device not directly connected to the multicast source, the interval of SRMs on its downstream interfaces is invalid.

3.3.4 MIB

Connected to other agents, the Simple Network Management Protocol (SNMP) manager uses information in the Management Information Base (MIB) to directly manage the PIM-DM function.

Working Principle

The MIB specifies variables (namely information that can be queried and set by the management process) maintained by network elements and directly manages the PIM-DM function.

Related Configuration

Enabling PIM-DM MIB

By default, the PIM-DM MIB function is enabled.

The **ip pim mib dense-mode** command is used to enable the PIM-DM MIB function.

3.4 Configuration

Configuration	Description and Command	
Configuring PIM-DM Basic Functions	(Mandatory) It is used to create the multicast service.	
	ip multicast-routing	Enables IPv4 multicast routing.
	ip pim dense-mode	Enables PIM-DM.
Configuring PIM-DM Neighbors	(Optional) It is used to limit the (S,G) pairs of legitimate multicast packets in Any Source Multicast (ASM) model.	
	ip pim query-interval *interval-seconds*	Sets the Interval of Hello messages on an interface.
	ip pim propagation-delay *interval-milliseconds*	Sets the prune propagation delay on an interface.
	ip pim override-interval *interval-milliseconds*	Sets the prune override interval on an Interface.
	ip pim neighbor-filter *access-list*	Configures neighbor filtering on an interface.
Configuring PIM-DM SRMs	**ip pim state-refresh disable**	Disables the processing and forwarding of SRMs.
	ip pim state-refresh origination-interval *interval-seconds*	Sets the Interval of SRMs on an interface.
Configuring PIM-DM MIB	**ip pim mib dense-mode**	Enables PIM-DM MIB.
Configuring PIM-DM PASSIVE mode	**ip pim dense-mode passive**	Enables PIM-DM PASSIVE mode.

3.4.1 Configuring PIM-DM Basic Functions

Configuration Effect

- Create a PIM-DM network and provide data sources and user terminals in the network with the IPv4 multicast service.

Notes

- PIM-DM needs to use the unicast routes existing in the network. Therefore, IPv4 unicast routing must be configured in the network.

Configuration Steps

Enabling IPv4 Multicast Routing

- Mandatory
- IPv4 multicast routing should be enabled on each router unless otherwise specified.

Enabling PIM-DM

- Mandatory
- PIM-DM should be enabled on the following interfaces unless otherwise specified: interconnected interfaces on routers and interfaces connecting multicast sources and user hosts.

Enabling the PIM-DM PASSIVE Function

- In a PIM network, if an interface needs to receive multicast packets without participating in the PIM network topology construction, the PIM-DM PASSIVE mode can be configured.
- If no special requirements are raised, enable the PIM-DM PASSIVE function on the following interfaces: interfaces of the stub network device in the multicast network for connecting to STAs. After the PIM-DM PASSIVE function is configured on an interface, the interface neither sends nor receives PIM packets.

Configuring the PIM-DM Sub VLAN Function

- In most scenarios on the PIM network, the PIM DM protocol does not need to be enabled on interfaces of a super VLAN. In general, a super VLAN includes many sub VLANs. If the PIM DM protocol is enabled on the interfaces of the super VLAN, multicast packets will be replicated and sent to all sub VLANs. As a result, traffic generated easily exceeds the device processing capability, causing protocol flapping. In some scenarios that require the PIM DM protocol to be enabled on the interfaces of the super VLAN, the PIM-DM sub VLAN function may be configured, to send packets to a specified sub VLAN or all sub VLANs.
- This function is available only on the interfaces of the super VLAN.

Verification

Make multicast sources send multicast packets and make user hosts join the groups.

- Check whether the user hosts can successfully receive packets from each group.
- Check whether correct PIM-DM routing entries are created on routers.

Related Commands

Enabling IPv4 Multicast Routing

Command	ip multicast-routing
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling PIM-DM

Command	ip pim dense-mode

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports(APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

Enabling PIM-DM PASSIVE Mode

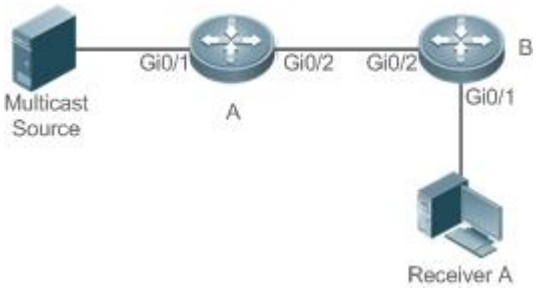
Command	**ip pim dense-mode passive**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports(APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

Displaying the PIM-DM Routing Table

Command	**show ip pim dense-mode mroute** [*group-or-source-address* [*group-or-source-address*]] [**summary**]
Parameter Description	*group-or-source-address*: Indicates a group address or source address. *group-or-source-address*: Indicates a group address or source address (The two addresses cannot be group addresses or source addresses at the same time). **summary**: Displays the routing table summary.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Check whether sufficient routing entries are provided. Check the upstream and downstream interface lists and ensure that a correct SPT tree is created.

Configuration Example

Enabling IPv4 Multicast Routing on the IPv4 Network

Scenario **Figure 3-3**	
Configuration Steps	● Configure IPv4 unicast routing protocols (for example, OSPF) on all the routers. ● Enable the IPv4 multicast routing function on all the routers. ● Enable the PIM-DM function on all the interconnected interfaces of the routers, Source, and Receiver..
A	`A# configure terminal` `A(config)# ip multicast-routing` `A(config)# interface GigabitEthernet 0/1` `A(config-if)# ip pim dense-mode` `A(config-if)# exit` `A(config)# interface GigabitEthernet 0/2` `A(config-if)# ip pim dense-mode` `A(config-if)# exit`
B	`B# configure terminal` `B(config)# ip multicast-routing` `B(config)# interface GigabitEthernet 0/1` `B(config-if)# ip pim dense-mode` `B(config-if)# exit` `B(config)# interface GigabitEthernet 0/2` `B(config-if)# ip pim dense-mode` `B(config-if)# exit`
Verification	Configure the multicast source (192.168.1.10) to send packets to G (229.1.1.1). Make Receiver A join G. ● Check whether the multicast packets from Source G are received by Receiver A. ● Check PIM-DM routing tables on Router A and Router B.
A	`A# show ip pim dense-mode mroute` `PIM-DM Multicast Routing Table` `(192.168.1.10, 229.1.1.1)`

	MRT lifetime expires in 182 seconds Source directly connected on GigabitEthernet 0/1 State-Refresh Originator State: Originator SRT:57, SAT:147 Upstream IF: GigabitEthernet 0/1 Upstream State: Forwarding Assert State: NoInfo Downstream IF List: GigabitEthernet 0/2, in 'olist': Downstream State: NoInfo Assert State: NoInfo
B	B# show ip pim dense-mode mroute PIM-DM Multicast Routing Table (192.168.1.10, 229.1.1.1) MRT lifetime expires in 130 seconds RPF Neighbor: 192.168.2.1, Nexthop: 192.168.2.1, GigabitEthernet 0/2 Upstream IF: GigabitEthernet 0/2 Upstream State: Forwarding Assert State: Loser, AT:125 Downstream IF List: GigabitEthernet 0/1, in 'olist': Downstream State: NoInfo Assert State: NoInfo

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

3.4.2 Configuring PIM-DM Neighbors

Configuration Effect

- Coordinate protocol parameters and adjust parameters in the Hello packet.

- Enable neighbor filtering to improve network security.

Notes

- Basic functions of PIM-DM must be configured.

Configuration Steps

- Set parameters on PIM router interfaces unless otherwise specified.

Verification

- Set parameters in a Hello packet on an interface and run the **debug ip pim dense-mode encode** command to check parameters.
- Enable neighbor filtering and run the **show ip pim dense-mode decode** command to display neighbor filtering information.
- Run the **show running-config interface** [*interface-type interface-number*] command to display configurations on an interface.

Related Commands

Setting the Interval of Hello Messages

Command	**ip pim query-interval** *interval-seconds*
Parameter Description	*interval-seconds*: The value ranges from 1 to 65,535 in the unit of seconds.
Command Mode	Interface configuration mode
Usage Guide	When the Hello interval is set, the holdtime value will be updated as its 3.5 times.

Every time when the interval of Hello messages is updated, the holdtime value is automatically updated as 3.5 times of the interval. If the result of the interval of Hello messages multiplied by 3.5 is greater than 65,535, the holdtime value is updated as 65,535.

Setting the Prune Propagation Delay

Command	**ip pim propagation-delay** *interval-milliseconds*
Parameter Description	*interval-milliseconds*: The value ranges from 1 to 32,767 in the unit of milliseconds.
Command Mode	Interface configuration mode
Usage Guide	Set **propagation-delay** of an interface, that is, configure the prune propagation delay of an interface.

Setting the Prune Override Interval

Command	**ip pim override-interval** *interval-milliseconds*
Parameter Description	*interval-milliseconds*: The value ranges from 1 to 32,767 in the unit of milliseconds.
Command Mode	Interface configuration mode
Usage Guide	Set **override-interval** of an interface, that is, configure the prune override time of an interface.

Configuring PIM-DM Neighbor Filtering

Command	**ip pim neighbor-filter** *access-list*
Parameter Description	*access-list*: The supported ACL ranges from 1 to 99. Naming an ACL is also supported.
Command Mode	Interface configuration mode
Usage Guide	Only addresses that meet ACL filtering conditions can be used as PIM neighbors of the current interface. Otherwise, the addresses filtered out cannot be neighbors. Peering refers to exchange of protocol packets between PIM neighbors. If peering with a PIM device is suspended, the neighbor relationship with it cannot be formed so that PIM protocol packets will not be received from the device.

Configuration Example

Configuring PIM-DM Neighbors on the IPv4 Network

Scenario **Figure 3-4**	
Configuration Steps	● Configure basic functions of PIM-DM (omitted). ● Set protocol parameters in a Hello packet on the Gi0/1 interface of device A.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if)# ip pim query-interval 60` `A(config-if)# ip pim propagation-delay 800` `A(config-if)# ip pim override-interval 1000` `A(config-if)# exit`

Verification	● Run the **show running-config interface** [*interface-type interface-number*] command to display configurations on an interface. ● Run the **debug ip pim dense-mode encode** command to debug parameters in a Hello packet.
A	`A# (config)#show running-config interface gigabitEthernet 0/1` `Building configuration...` `Current configuration : 245 bytes` `!` `interface GigabitEthernet 0/1` ` ip pim dense-mode` ` ip pim query-interval 60` ` ip pim propagation-delay 800` ` ip pim override-interval 1000`
	`A# debug ip pim dense-mode encode` `*Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Hold-Time 210` `*Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Gen-ID 1362200073` `*Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello PD=800 ms, OI=1000 ms` `*Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello SR-Interval 60` `*Dec 22 15:00:58: %7: [ENCODE] Enc Msg Hdr: Hello Checksum=65396, MsgLen=34 Assert State: Loser, AT:125`

Configuring PIM-DM Neighbor Filtering on the IPv4 Network

Scenario **Figure 3-5**	
Configuration Steps	● Configure basic functions of PIM-DM (omitted). ● Configure an ACL on device A. ● Configure PIM neighbor filtering on the Gi0/1 interface of device A.
A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if)# ip pim query-interval 60`

	A(config-if)# ip pim propagation-delay 800 A(config-if)# ip pim override-interval 1000 A(config-if)# exit
Verification	● Run the **show running-config interface** [*interface-type interface-number*] command to display configurations on the interface. ● Run the **debug ip pim dense-mode decode** command to debug parameters in a Hello packet.
A	A#show running-config interface gigabitEthernet 0/2 Building configuration... Current configuration : 187 bytes ! interface GigabitEthernet 0/1 ip pim dense-mode ip pim neighbor-filter pim-dm
	A# debug ip pim dense-mode decode Dec 22 15:15:47: %7: [DECODE] Dec Msg: PIM Hello message, version 2 Dec 22 15:09:47: %7: [DECODE] Dec Msg: Neighbor 192.168.2.2/32 on GigabitEthernet 0/1 denied by access-list pim-dm

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

3.4.3 Configuring PIM-DM SRMs

Configuration Effect

- Enable or disable the PIM-DM SRM function.
- Adjust the interval of SRMs.

Notes

- Basic functions of PIM-DM must be configured.

Configuration Steps

- The interval of SRMs is only applicable only to the PIM router interfaces that are directly connected to the multicast source.

Verification

- Configure the PIM-DM SRMs and run the **show running-config** command to display the SRM status.
- Run the **show ip pim dense-mode track** command to display the SRM number.
- Run the **show running-config interface** [*interface-type interface-number*] command to display interface configurations.

Related Commands

Disabling the Processing and Forwarding of SRMs

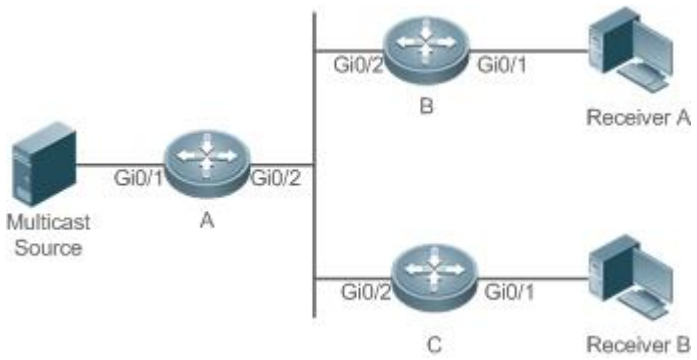
Command	**ip pim state-refresh disable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When the processing and forwarding of SRMs are disabled, the State Refresh Capable option is not included in a Hello packet, and is not processed when the Hello packet is received. Disabling the SRM function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, it is recommended not to disable this function in general conditions.

Setting the Interval of SRMs

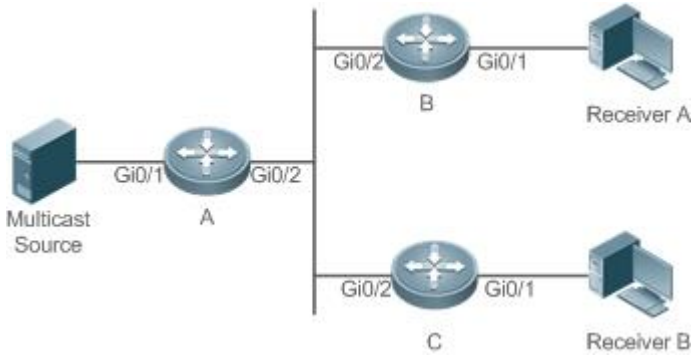
Command	**ip pim state-refresh origination-interval** *interval-seconds*
Parameter Description	*interval-seconds*: The value ranges from 1 to 100 in the unit of second.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Disabling the Processing and Forwarding of SRMs on an Interface on the IPv4 Network

Scenario **Figure 3-6**	
Configuration Steps	● Configure basic functions of PIM-DM (omitted). ● Disable processing and forwarding of a PIM-DM SRM on an Interface of device A.
A	`A# configure terminal` `A(config)# ip pim state-refresh disable`
Verification	● Run the **show running-config** command to check the configuration.
A	`A# (config)# show running-config` `…` `!` `ip pim state-refresh disable` `!` `…`

Setting the Interval of SRMs on the IPv4 Network

Scenario **Figure 3-7**	
Configuration Steps	● Configure basic functions of PIM-DM (omitted). ● Set the interval of PIM-DM SRMs on the Gi0/1 interface of device A.

A	`A# configure terminal` `A(config)# interface GigabitEthernet 0/1` `A(config-if)# ip pim state-refresh origination-interval 5` `A(config-if)# exit`
Verification	● Run the **show running-config interface** [*interface-type interface-number*] command to display interface configurations. ● Run the **show ip pim dense-mode track** command to display the SRM number.
A	`A#show running-config interface gigabitEthernet 0/1` `Building configuration...` `Current configuration : 201 bytes` `!` `interface GigabitEthernet 0/1` ` ip pim dense-mode` ` ip pim state-refresh origination-interval 5`
	`A #show ip pim dense-mode track` `PIM packet counters` `Elapsed time since counters cleared: 00:18:54` `received sent` `Valid PIMDM packets: 38 102` `Hello: 38 76` `Join/Prune: 0 0` `Graft: 0 0` `Graft-Ack: 0 0` `Assert: 0 0` `State-Refresh: 0 26` `PIM-SM-Register: 0` `PIM-SM-Register-Stop: 0` `PIM-SM-BSM: 0` `PIM-SM-C-RP-ADV: 0`

	Unknown Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Unknown PIM version: 0 Send errors: 0

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

3.4.4 Configuring PIM-DM MIB

Configuration Effect

- Enable the MIB function for PIM-DM.

Verification

- Configure the MIB function of PIM-SM and run the **show running-config** command to check whether the function is configured.

Related Commands

Enabling PIM-DM MIB

Command	**ip pim mib dense-mode**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

3.5 Monitoring

Clearing

Description	Command

Resets the statistic start time and clears the counters of PIM-DM packets.	**clear ip pim dense-mode track**

Displaying

Description	Command
Displays the help information of the commands with IP PIM as the key word.	**ip pim help**
Displays PIM-DM information of an interface.	**show ip pim dense-mode interface** [*interface-type interface-number*] [**detail**]
Displays the PIM-DM neighbors.	**show ip pim dense-mode neighbor** [*interface-type interface-number*]
Displays the PIM-DM next-hop information.	**show ip pim dense-mode nexthop**
Displays the PIM-DM routing table.	**show ip pim dense-mode mroute** [*group-or-source-address* [*group-or-source-address*]] [**summary**]
Displays the number of PIM-DM packets sent and received since the statistic start time.	**show ip pim dense-mode track**

4 Configuring PIM-SM

4.1 Overview

Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol.

A multicast source sends a packet to a group address. The packet is forwarded by network devices hop by hop and finally reaches the group members. On Layer-3 network devices, PIM is used to create and maintain multicast routing entries, so as to support multicast forwarding.

PIM works in two modes: Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM is applicable to large-scale networks where group members are sparsely distributed in a wide scope.
- PIM-DM is applicable to small networks where group members are densely distributed.

Protocols and Standards

- RFC4601: Protocol Independent Multicast -Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC3962: Protocol Independent Multicast - Dense Mode protocol
- RFC4607: Source-Specific Multicast for IP

4.2 Applications

Application	Description
Enabling ASM for PIM-SM	The receiver receives any multicast source.
Enabling SSM for PIM-SM	The receiver receives only a specific multicast source.

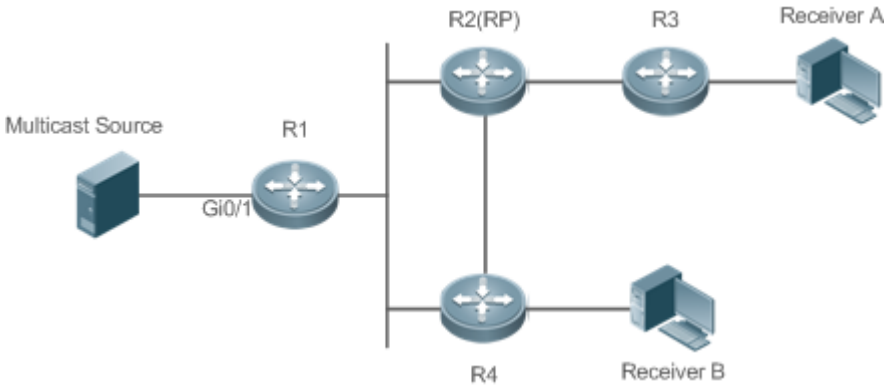
4.2.1 Enabling ASM for PIM-SM

Scenario

Provide multicast services within only one domain.

For example, in the following figure, the receiver receives any multicast source.

Figure 4-1



Remarks	R 1 is connected directly to the multicast source. R 2 serves as the rendezvous point (RP). R 3 is connected directly to Receiver A. R 4 is connected directly to Receiver B.

Deployment

- Run the Open Shortest Path First (OSPF) protocol to realize unicast routing.
- Run PIM-SM to realize multicast routing.
- Run the Internet Group Management Protocol (IGMP) in the network segment of the user host to manage group members.

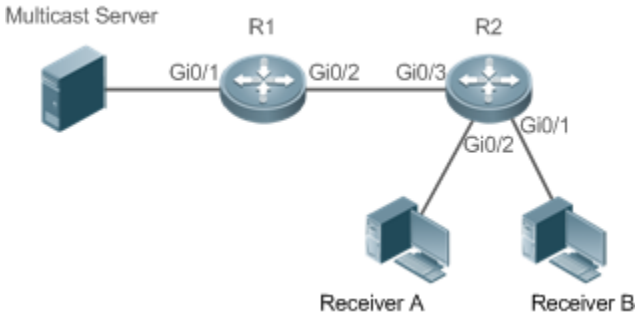
4.2.2 Enabling SSM for PIM-SM

Scenario

Provide multicast services within only one domain.

For example, in the following figure, the receiver receives a specific multicast source.

Figure 4-2



Remarks	R 1 is connected directly to the multicast source. R 2 serves as the RP.

	R 2 is connected directly to Receiver A. R 2 is connected directly to Receiver B.

Deployment

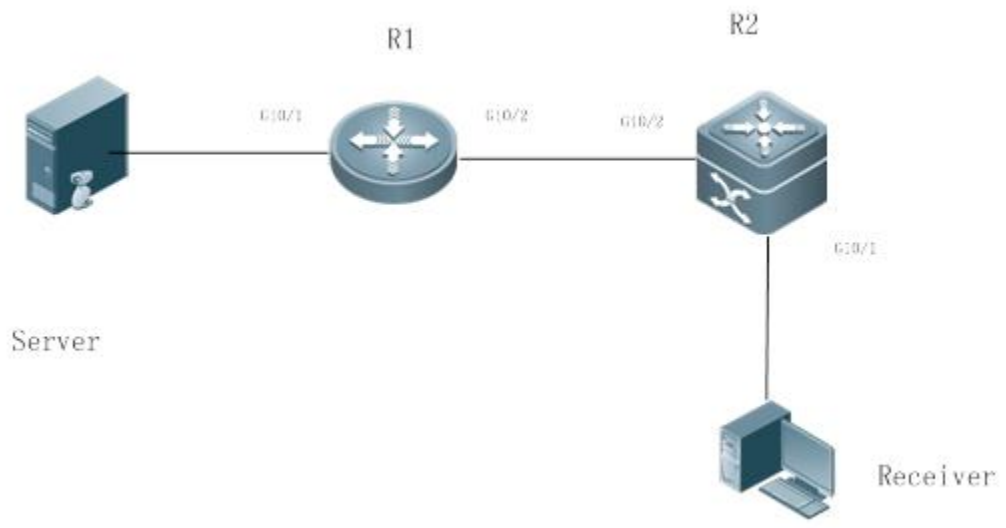
- Run the OSPF protocol to realize unicast routing.
- Run PIM-SM to realize multicast routing.
- Run the source-specific multicast (SSM) of PIM-SM within the domain.
- Run IGMPv3 in the network segment of the user host to manage group members.

4.2.3 PIM-DM Application in a Hot Backup Environment

Scenario

In a hot backup environment, run PIM-DM. A device performs hot backup switching to ensure that traffic is not interrupted.

Figure 4-1



Remarks	R1 is connected to the video server, R2 is directly connected to the receiver, and R2 runs in hot backup mode. A Layer-3 multicast protocol runs on R1 and R2.

Deployment

- Run OSPF on R1 and R2 to implement unicast routing.
- Run PIM-DM on R1 and R2 to implement multicast routing.
- Make R2 run in a hot backup environment.

Remarks	R2 may perform hot backup switching in the hot backup environment. In this case, the query interval of PIM Hello packets (the default value is 30 seconds) needs to be adjusted on R2 because the keepalive timer of the neighbor in PIM Hello packets of R1 may have expired (the default value is 3.5 times the query interval, that is, 105 seconds). The multicast function relies on the unicast function currently, and the multicast function starts convergence after the unicast function convergence is complete. For example, the default graceful restart (GR) convergence time of the unicast function is 120 seconds. It is recommended that the query interval of PIM Hello packets be set to 60 seconds. The keepalive time of the neighbor in PIM Hello packets is 210 seconds. In this scenario, the query interval of PIM Hello packets need to be set with a reference to the GR convergence time of the unicast function and the value of 3.5 times the query interval of PIM Hello packets must be larger than the GR convergence time of the unicast function. In a hot backup environment, it is recommended that the query interval of PIM Hello packets be larger than the default value (30 seconds). Otherwise, the keepalive timer of the neighbor in PIM Hello packets of the peer end times out during hot backup switching.

4.3 Features

Basic Concepts

PIM Router and PIM Interface

A router running PIM is called a PIM router. An interfaces running PIM is called a PIM interface.

Multicast packets are forwarded on PIM routers. The PIM interfaces where multicast packets are received are called upstream interfaces, and the PIM interfaces where multicast packets are sent are called downstream interfaces.

The network segments where upstream interfaces are located are called upstream network segments, and the network segments where downstream interfaces are located are called downstream network segments.

PIM Network and PIM Domain

PIM routers are connected through PIM interfaces to form a PIM network.

On some PIM interfaces, borders can be set to divide a large PIM network into multiple PIM domains. The borders can reject the passage of specific multicast packets or limit the transmission of PIM packets.

Multicast Distribution Tree, DR, and RP

Multicast packets are transmitted from one point to multiple points, forming a tree-shaped forwarding path. Such forwarding path is called the multicast distribution tree (MDT), which includes the following two types:

- RP Tree (RPT): It is rooted at an RP, and uses the designated router (DR) of the member groups connected to it as its leaves.
- Shortest path tree (SPT): It is rooted at a DR that is connected to the multicast source, and uses the RP or the DR of the member groups connected to it as its leaves.

Both the DR and RP are the functions of a PIM router.

- An RP collects the information of a multicast source or multicast member on the network.

- The DR connected to the multicast source advertises the multicast source information to the RP; the DR connected to multicast group members advertises the information of multicast group members to the RP.

(*, G), (S, G)

- (*, G): Indicates the packets sent from any source to a group (G), the corresponding route entries, and the RPT.
- (S, G): Indicates the packets sent from the source (S) to a group (G), the corresponding routing entries, and the SPT.

ASM, SSM

PIM-SM supports both any-source multicast (ASM) and SSM, and it is applicable to different multicast group address segments.

- ASM: In this model, a user is not allowed to select a multicast source. The user host joins a group, and receives the packets sent from all sources.
- SSM: In this model, a user can select a multicast source. The user host joins a group and specifies the source address. Then only the packets sent from this source address is received.

Requirements for using an SSM model: Before selecting a multicast source, you need to learn the address of the multicast source using other network services.

Overview

Feature	Description
PIM-SM Neighbor	Establishes neighbor relationships between RIM routers to form a PIM network.
DR Election	In the network segment where group member hosts are located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the group members. In the network segment where the multicast source is located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the multicast source.
BSR Mechanism	On a PIM network, the BSR generates periodic candidate RPs and bootstrap packets of corresponding group addresses.
RP Mechanism	On a PIM network, through static RP configuration or dynamic RP election, the location of the RP can be learned by each PIM router.
Register Information of the Multicast Source	When the multicast source is detected on the network, the source DR sends a register packet to the RP, which obtains the source information and multicast packet.
Creating an RPT	When a group member is detected on the network, the DR connecting to the group members send packets toward the RP to form an RPT. If the multicast source already exists on the network, the packets arrived at the RP can be sent to the group members along the RPT.
Creating an SPT	When data packets arrive at the DR connecting to group members, the DR sends these packets toward the multicast source to form an SPT, and multicast packets are sent to group members along the SPT.

Feature	Description
ASM and SSM	A PIM router can provide multicast services of both ASM model and SSM model at the same time. SSM model applies to the groups whose addresses are within the range of the SSM addresses. For other groups, use ASM model.

4.3.1 PIM-SM Neighbor

Neighbor relationships are established between PIM routers to form a PIM network. Neighbor relationships must be established between PIM routers before PIM control packets can be exchanged or multicast packets can be forwarded.

Working Principle

A PIM interface sends a Hello packet. For the IPv4 multicast packet whose Hello packet is encapsulated, the destination address is 224.0.0.13 (indicating all PIM routers in the same network segment), the source address is the IP address of the PIM interface, and the Time To Live (TTL) value is 1. For the IPv6 multicast packet whose Hello packet is encapsulated, the destination address is ff02::d.

A Hello packet is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.

↘ Discovering Neighbors

PIM routers in the same network segment receive multicast packets from the destination address 224.0.0.13. In this way, the PIM routers obtain neighbor information and establish neighbor relationships.

When a PIM interface is enabled or detects a new neighbor, a triggered-hello-delay packet is used to generate a random time. Within the time, the interface sends Hello packets.

↘ Coordinating Protocol Parameters

A Hello packet includes multiple protocol parameters, which are described as follows:

– DR_Priority: indicates the priority of a router interface for competing for the DR. A higher priority means a higher chance of winning.

– Holdtime: Indicates the time in which a neighbor is held in the reachable state

– LAN_Delay: Indicates the LAN delay for transmitting a Prune packet in a shared network segment.

– Override-Interval: Indicates the prune override time carried in a Hello packet.

When a PIM router receives a Prune packet from an upstream interface, it indicates that downstream interfaces exist in the shared network segment. If the PIM router still needs to receive multicast data, the PIM router must sent a Prune Override packet to the upstream interface within the override interval.

LAN_Delay + Override Interval = PPT (Prune-Pending Timer). After a PIM router receives a Prune packet from a downstream interface, the PIM router will not immediately perform pruning until PPT times out. Within the time of PPT, if the PIM router receives a Prune rejection packet from the downstream interface, the PIM router cancels pruning.

↘ Maintaining Neighbor Relationships

A Hello packet is sent periodically between PIM routers. If a Hello packet is not received from a PIM neighbor within Holdtime, the neighbor is considered unreachable and is deleted from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an upstream or downstream neighbor in an MDT is unreachable, multicast routes converge again and the MDT is reshaped.

Related Configuration

Enabling PIM-SM on an Interface

By default, PIM-SM is disabled on an interface.

Run **ip pim sparse-mode** to enable or disable PIM-SM on an interface.

PIM-SM must be enabled on an interface to involve the interface in the PIM protocol. If PIM-SM is not enabled for the interface of a DR, static RP, candidate RP (C-RP), or candidate BSR (C-BSR), corresponding roles of the PIM protocol cannot be run.

Setting the Interval of Hello Packets on an Interface

By default, a Hello packet is sent every 30s.

Run **ip pim query-interval** *interval-seconds* to adjust the interval of Hello packets. The value ranges from 1 to 65, 535.

A Hello packet is transmitted less frequently when the value of *interval-seconds* is greater.

4.3.2 DR Election

In the network segment where group member hosts are located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the group members.

In the network segment where the multicast source is located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the multicast source.

The DR sends Join/Prune packets toward the MDT, or sends the multicast source data to the MDT.

Working Principle

When creating a PIM neighbor, you can send a Hello packet to obtain the IP address and DR priority of the neighbor to elect a DR.

Two parameters play a key role in winning the DR election: the DR priority of an interface and the IP address of the interface.

DR Priority of an Interface

During the DR election, the RIM router with the highest DR priority will be elected as the DR.

Interface IP Address

During the DR election, if the priority of interfaces is the same, then interface IP addresses will be compared. The interface with the maximum IP address will be elected as the DR.

Related Configuration

Enabling PIM-SM on an Interface

By default, PIM-SM is disabled on an interface.

Run **ip pim sparse-mode** to enable or disable PIM-SM on an interface.

PIM-SM must be enabled on an interface to involve the interface in the PIM protocol. If PIM-SM is not enabled for the interface of a DR, static RP, C-RP, or C-BSR, corresponding protocols cannot be run.

Adjusting the DR Priority of an Interface

By default, the DR priority is 1.

Run **ip pim dr-priority** *priority-value* to adjust the DR priority of the interface. The value ranges from 0 to 4,294,967,294.

The DR priority is used in the DR election in the network segment directly connected the interface. A greater value indicates a higher priority.

4.3.3 BSR Mechanism

On a PIM network, the BSR generates periodic candidate RPs and bootstrap packets of corresponding group addresses. These bootstrap packets are sent hop by hop in the domain. All the routers on the entire network will receive these bootstrap packets, and record these candidate RPs and their corresponding group addresses.

Working Principle

One or multiple candidate BSRs are configured in a PIM-SM domain. You need to apply a certain algorithm to select the BSR from these candidate BSRs.

Related Configuration

Configuring Candidate BSRs

By default, candidate BSRs are not configured.

Run **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]] to configure or cancel the configuration of candidate BSRs.

Through bootstrap packet (BSM) learning and competition of candidate BSRs, a unique BSR is generated for the PIM-SM domain.

Configuring BSR Boarders

By default, BSR boarders are not configured.

Run **ip pim bsr-border** to configure or cancel the configuration of BSR boarders.

After this command is configured, BSMs received by the interface will be discarded and will not be forwarded by this interface, preventing BSM flooding.

Filtering BSMs

By default, BSMs from the BSR are not filtered.

Run **ip pim accept-bsr list** { <1-99> | <1300-1999> | *WORD* } to configure whether to filter BSMs.

If this function is enabled, only legible BSMs are received by the interface; if this function is disabled, all the external BSMs will be received by the device running PIM-SM.

↘ Configuring Legible C-RP Addresses and the Multicast Groups They Serve for a Candidate BSR

By default, Candidate-RP-Advertisement (C-RP-Adv) packets are not filtered by a candidate BSR.

Run **ip pim accept-crp list** { *<100-199>* | *<2000-2699>* | *WORD* } to configure whether to filter C-RP-Adv packets.

If this function is enabled, C-RP addresses and corresponding multicast groups are filtered by a candidate BSR. If this function is disabled, all external C-RP-Adv packets are received by a candidate BSR.

↘ Allowing a C-BSR to Receive a C-RP-ADV Packet Whose Prefix-Count Is 0

By default, a candidate BSR cannot receive a C-RP-ADV packet whose prefix-count is 0.

Run **ip pim accept-crp-with-null-group** to configure whether to receive a C-RP-ADV packet whose prefix-count is 0.

If this function is enabled, a C-RP-ADV packet whose prefix-count is 0 can be received by a candidate BSR. If this function is disabled, a C-RP-ADV packet whose prefix-count is 0 cannot be received by a candidate BSR.

4.3.4 RP Mechanism

On a PIM network, through static RP configuration or dynamic RP election, the location of the RP can be learned by each PIM router. The RP as the root of the RPT, is the point where the RPT is rooted at and RPT data traffic is forwarded from.

Working Principle

All PIM routers in the same PIM domain must be mapped to the same RP as a specific multicast group address. On a PIM network, an RP can be configured as static or dynamic.

↘ Static RP

In static RP configuration, RP addresses are configured directly on PIM routers and these addresses are learnt by the entire PIM network.

↘ Dynamic RP

In a PIM-SM domain, there are candidate RPs that send unicast packets (including RP addresses and the multicast groups they serve) to the BSR, which generates periodic candidate RPs and bootstrap packets of corresponding group addresses. These bootstrap packets are sent hop by hop in the domain, and received and saved by PIM routers, which apply a hash function to map the group addresses to the candidate RP that can provide services. Then the RP corresponds to these multicast group addresses can be confirmed.

Related Configuration

↘ Configuring Static RP Addresses

By default, no RP address is configured.

Run **ip pim rp-address** *rp-address* [*access-list*] to configure a static RP address for a PIM router.

To use static RP addresses, the static RP address of all routers in the PIM-SM domain must be the same, so that the PIM SM multicast routing remains consistent.

↘ Configuring Candidate C-RP Addresses

By default, no C-RP address is configured.

Run **ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access-list*] to configure or cancel a PIM router as a candidate C-RP.

After a candidate RP is configured, it can send periodic C-RP-Adv packets to the BSR, and the information carried by these C-RP-Adv packets will be advertized to all PIM-SMs in the domain, ensuring the uniqueness of RP mapping.

↘ Ignoring the RP Priority in RP-Set

By default, C-RP of the highest priority is configured.

Run **ip pim ignore-rp-set-priority** to select or deselect the RP priority when selecting the corresponding RP of a multicast group.

If you want to select an RP from multiples RPs that serve the same multicast group address, you can run this command to ignore the RP priority. If this command is not configured, RP priority will be considered when two RPs are compared.

4.3.5 Register Information of the Multicast Source

When the multicast source is detected on the network, the source DR sends a register packet to the RP, which obtains the source information and multicast packet.

Working Principle

When a source DR receives a multicast packet from the host directly connected to it, the source DR encapsulates the multicast packet into the register packet, and sends the unicast packet to RP to form an (S, G) entry.

If the RP has an outgoing interface for the forwarding entry, it encapsulates the data packet and forwards the packet to the outgoing interface.

If the RP does not have the forwarding entry of the present group, it generates the (S, G) entry and enables the timer. If the timer times out, the RP sends a Register-Stop packet to the DR to delete the entry. The source DR sends an inspection packet before timeout after it receives the Register-Stop packet.

If no Register-Stop packet is received by the DR, the DR on the timeout data source will encapsulate the multicast data in the register packet and send the unicast packet to the RP.

If a Register-Stop packet is received by the DR, time-delay will be performed once again, and an inspection packet will be sent before time delay.

Related Configuration

Detecting the Reachability of a Register Packet

By default, the reachability of an RP is not detected.

Run **ip pim register-rp-reachability** to configure or cancel the detection of the reachability of an RP.

You can enable this function if you want to detect whether an RP is reachable for a register packet sent from a DR. After this function is enabled, the DR will detect the reachability of a register packet before it is sent to an RP, namely, the DR will check whether a route to the RP exists in the unicast routing entry and static multicast routing entry. If the route does not exist, the register packet will not be sent.

Configuring an RP to Filter the Addresses of Register Packets

By default, all register packets are received an RP.

Run **ip pim accept-register** { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *access-list*] } to configure an RP to filter or cancel the filtering of the source addresses of received register packets.

You can run this command if you want to filter the source addresses of received register packets. If this function is not enabled, all register packets will be received by the RP. If this function is disabled, only the register packets whose source addresses and multicast group addresses included in access control lists (ACLs) are processed; otherwise, the packets will be filtered.

Limiting the Speed for Sending a Register Packet

By default, the speed for sending a register packet is not limited.

Run **ip pim register-rate-limit** *rate* to limit or cancel the limitation of the speed for sending a register packet.

If the **no** form of this command is configured, the speed is not limited. This command takes effect for only the register packet of each (S, G) packet, but not all the register packets in the entire system.

Calculating the Checksum of the Entire Register Packet Length

By default, the checksum of a register packet is calculated as stipulated by the protocol.

Run **ip pim register-checksum-wholepkt** [**group-list** *access-list*] to configure the checksum of the register packet length.

You can enable this function if you want to include the length of encapsulated multicast packets into the checksum of the register packet length. If this function is disabled, the checksum of a register packet is calculated as stipulated by the protocol.

Configuring an RP to Forward Multicast Data Packets to Downstream Interfaces After Decapsulating Register Packets

By default, register packets are not decapsulated and multicast packet are not forwarded to interfaces.

Run **ip pim register-decapsulate-forward** to forward or cancel the forwarding of data packets to downstream interfaces.

You can run this command if you want to decapsulate a register packet and forward the multicast packet. If this function is disabled, the multicast packet will not be forwarded.

Configuring the Source IP Address of a Register Packet

By default, the source IP address of a register packet is the same as the interface address of the DR connected to the multicast source.

Run **ip pim register-source** { *local_address* | *Interface-type interface-number* } to configure the source IP address.

You can run this command is you want to configure the source IP address of the register packet sent by a DR. If this function is disabled or the **no** form of this command is used, the source address of the register packet will be the same as the interface address of the DR connected to the multicast source. If you want to configure *local_address*, the configured address must be reachable for a unicast route. *Interface-type interface-number* can be a typical a loopback interface or an interface of other types. The interface address must have been advertised by a unicast route.

Configuring the Suppression Time of a Register Packet

By default, the suppression time of a register packet is 60s.

Run **ip pim register-suppression** *seconds* to configure the suppression time.

If you run this command on a DR, you can change the suppression time of the register packets sent from the DR. If you run this command but does not run **ip pim rp-register-kat** on an RP, the keepalive period of the RP will be changed.

Configuring the Inspection Time of a Null Register Packet

By default, the inspection time is 5s.

Run **ip pim probe-interval** *interval-seconds* to configure the inspection time.

In the time interval before the timeout of register packet suppression, the source DR can send a null register packet to an RP. This time interval is called the inspection time, which is 5s by default.

Configuring the Time of a RP KAT

By default, the default value of a keepalive timer (KAT) is used. The default value is calculated as follows: Suppression time of a register packet x 3 + Inspection time of a null register packet.

Run **ip pim rp-register-kat** *seconds* to configure the KAT time.

You can run this command if you want to configure the keepalive time of (S, G) of a register packet sent from an RP.

4.3.6 Creating an RPT

When a group member is detected on the network, the DR connecting to the group members send packets toward the RP to form an RPT. If the multicast source already exists on the network, the packets arrived at the RP can be sent to the group members along the RPT.

Working Principle

To create an RPT, perform the following steps:

A receiver DR receives an IGMP (*, G) include report packet from the receiving end.

If the DR is not the RP of this group (G), the DR will send a (*, G) Join packet toward the RP. The router receiving this (*, G) Join packet will send the packet hop by hop until it is received by the RP, which means that the RP has joined the RPT.

When the data source host sends the multicast data to a group, the source data is encapsulated in the register packet, and sent from the source DR to the RP in unicast mode. Then the RP decapsulates the register packet, takes the data packets out, and forwards these packets to each group member along the RPT.

The RP sends the (S, G) Join packets along the data source to join the SPT of this source.

After the SPT between the RPs to the source DR is created, the data packets from the data source will be sent decapsulated to the RPs along the SPT.

When the first multicast data packet arrives at an RP along the SPT, the RP sends a Register-Stop packet to the source DR to stop sending a register packet. After the source DR receives the Register-Stop packet, it stops encapsulating a register packet and sends the packet along the SPT to the RP, which will forwards the packet to each group member.

Related Configuration

↘ Configuring the Interval for Sending a Join/Prune Packet

By default, the interval for sending a Join/Prune packet is 60s.

Run **ip pim jp-timer** *seconds* to configure the interval for sending a Join/Prune packet.

You can run this command to configure the interval for sending a Join/Prune packet. If not configured, the value will be a default 60s.

4.3.7 Creating an SPT

When data packets arrive at the DR connecting to group members, the DR sends these packets toward the multicast source to form an SPT, and multicast packets are sent to group members along the SPT. In this way, the burden on RP in the RPT is reduced, and the source DR will arrive at the receiver DR with less hops.

Working Principle

To create an SPT, perform the following steps:

The receiver DR sends (*, G) Join packets toward the source DR along the SPT, and (*, G) Join packets are then send hop by hop until they are received by the source DR, forming an SPT.

Related Configuration

By default, SPT switchover is not enabled.

Run **ip pim spt-threshold** [**group-list** *access-list*] to configure whether to switch to an SPT.

If this function is enabled, upon the reception of the first (S, G) packet, a PIM Join packet is triggered, and an SPT is created. If **group-list** is specified, all the specified groups will be switched to the SPT. If the **no** form of this command is used and **group-list** is not specified, an RPT will not be switched to an SPT, and the DR will remain in the RPT and send a Prune

packet toward the source DR; if the **no** form of this command is used and **group-list** is specified, and that the ACLs have been configured, it means that the association between **group-list** and the ACLs is canceled, and all the groups are allowed to switch from an RPT to an SPT.

4.3.8 ASM and SSM

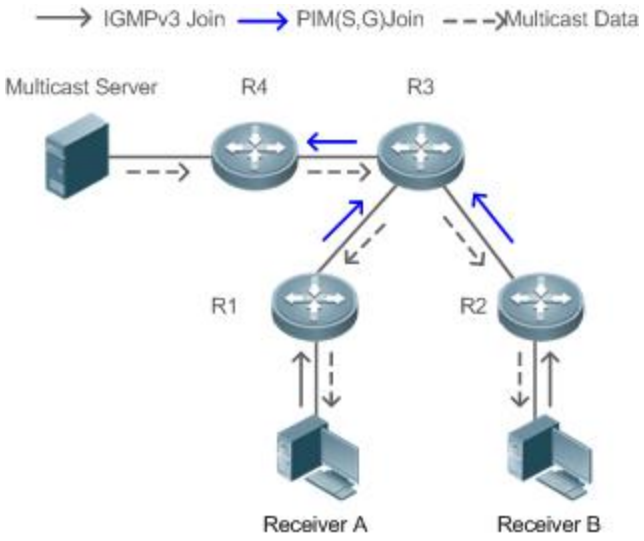
A PIM router can provide multicast services of both ASM model and SSM model at the same time. SSM model applies to the groups whose addresses are within the range of the SSM addresses. For other groups, use ASM model. In an ASM model, only the multicast group (G) is specified for a multicast receiver, and the multicast source (S) is not specified. In an SSM model, both the multicast source (S) and multicast group (G) can be specified for a multicast receiver.

Working Principle

⚠ To realize SSM in an IPv4 router, IGMPv3 needs to be applied for managing membership between the host and devices, and PIM-SM needs to be applied to connect to devices.

In an SSM model, as a multicast receiver has learnt the (S, G) of the multicast source through a certain channel (for example, by visiting the server or receiving an advertisement), when a multicast receiver needs to request a multicast service, the multicast receiver can send the IGMP (S, G) Join packet toward the router of last hop. For example, as shown in Figure 4-3, the multicast receiver 1 sends the IGMP (S, G) Join packet to request the multicast service (S, G). After the router of last hop receives the IGMP (S, G) Join packet, it sends the PIM (S, G) Join packet to the multicast source hop by hop. As shown in Figure 4-3, when R 1 receives the IGMP (S, G) Join packet sent from multicast Receiver 1, R 1 sends the PIM (S, G) Join packet to R 3, which then sends the packet to R 4, thereby forming an SPT connecting the multicast receiver and multicast source.

Figure 4-3 SSM Model



To create an SSM model, the following requirements need to be met:

- A multicast receiver needs to learn the (S, G) of the multicast source in advance, and an IGMP (S, G) Join packet needs to be sent if the receiver needs to request a multicast service.

- IGMPv3 must be run on the interface of the last hop router connecting to the multicast receiver. IGMPv1 and IGMPv2 does not support SSM.
- PIM-SM and SSM must be run on the devices connecting the multicast receiver and multicast source.

⚠ The default range of SSM groups is 232/8. You can run a command to change the value.

An SSM has the following features:

- A multicast receiver can learn the information of the multicast source through a certain channel (for example, by visiting the server or receiving an advertisement) in advance.
- An SSM model is a specific subnet of PIM-SM. It handles only the PIM (S, G) Join and PIM (S, G) Prune packets and discards the RPT-related packets, for example, PIM (*, G) Join/Prune packets, that are within the scope the SSM. If the SSM detects a register packet within the scope, it will respond immediately with a Register-Stop packet.
- If an RP is not required, the election and distribution of RP information are not performed. The MDTs in an SSM are all SPTs.

Related Configuration

ASM is enabled by default.

Run **ip pim ssm** { **default** | **range** *access-list* } to configure whether to switch to SSM.

In SSM, multicast packets can be received by the multicast source directly but not along the RP tree.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic PIM-SM Functions	⚠ (Mandatory) It is used to configure the multicast service.	
	ip multicast-routing	Enables IPv4 multicast routing.
	ip pim sparse-mode	Enables PIM-SM.
	ip pim rp-address	Configures a static RP.
	ip pim rp-candidate	Configures a C-RP.
	ip pim bsr-candidate	Configures a C-BSR.
	ip pim ssm	Enables SSM.
Configuring PIM-SM Neighbors	⚠ (Optional) It is used to configure the parameters for sending and receiving the Hello packets between neighbors.	
	ip pim query-interval *interval-seconds*	Configures the interval for sending Hello packets.
	ip pim propagation-delay *milliseconds*	Configures the prune propagation delay.
	ip pim override-interval *milliseconds*	Configures the prune override interval.

Configuration	Description and Command	
	ip pim neighbor-tracking	Enables the suppression capability of an interface for sending Join packets.
	ip pim triggered-hello-delay *interval-seconds*	Configures the delay for sending Hello packets.
	ip pim dr-priority *priority-value*	Configures the DR priority of a Hello packet.
	ip pim neighbor-filter *access_list*	Configures neighbor filtering.
Configuring BSR Parameters	(Optional) It is used to configure a BSR.	
	ip pim bsr-border	Configures BSR boarders.
	ip pim accept-bsr list { <1-99> | <1300-1999> | *WORD* }	Configures BSM packets limit on a PIM router.
	ip pim [**vrf** *vid*] **accept-crp list** *access-list*	Configures a C-BSR to inspect the address range of a C-PR.
Configuring RP and DR Parameters	(Optional) It is used to configure the parameters of an RP or a DR.	
	ip pim ignore-rp-set-priority	Ignores the C-RP priority.
	ip pim register-rp-reachability	Enables the source DR to detect the RP reachability.
	ip pim accept-register list *access-list*	Configures the range of source register (S, G) addresses.
	ip pim register-rate-limit *rate*	Limits the speed for sending register packets.
	ip pim register-checksum-wholepkt [**group-list** *access-list*]	Calculates the checksum of the entire register packet.
	ip pim register-decapsulate-forward	Enables an RP to decapsulate a register packet and forwards the multicast packet to interfaces.
	ip pim register-source { *local_address* | *Interface-type interface-number* }	Configures the source IP address of a register packet.
	ip pim register-suppression *seconds*	Configures the suppression time of a register packet.
	ip pim probe-interval *seconds*	Configures the inspection time of a null register packet.
	ip pim rp-register-kat *seconds*	Configures the interval of KATs on an RP.

Configuration	Description and Command	
Configuring the Interval for Sending a Join/Prune Packet	(Optional) It is used to specify the interval for sending a Join/Prune packet.	
	ip pim jp-timer *seconds*	Configures the interval for sending a Join/Prune packet.
Configuring the Router of Last Hop to Switch from an RPT to SPT	(Optional) It is used to switch from SPT to RPT.	
	ip pim spt-threshold [**group-list** *access-list*]	Enables SPT switchover.
Configuring PIM-DM PASSIVE mode	(Optional) It is used to configure the interface of the stub router connected to the host.	
	ip pim sparse-mode passive	Enables PIM-DM PASSIVE mode.

4.4.1 Configuring Basic PIM-SM Functions

Configuration Effect

- Create a PIM-SM network and provide data sources and user terminals on the network with the IPv4 multicast service.
- Any of ASM or SSM or both models can be configured.

Notes

- PIM-SM needs to use existing unicast routes on the network. Therefore, IPv4 unicast routes must be configured on the network.
- If the PIM network needs to support SSM multicast services, IGMPv3 or SSM mapping must be configured.

Configuration Steps

Enabling IPv4 Multicast Routing

- Mandatory.
- If not specified, IPv4 multicast routing must be enabled on each router.

Enabling PIM-SM

- Mandatory.
- If not specified, PIM-SM must be enabled on the following interfaces: interconnecting router interfaces, interfaces of static RPs, C-RPs, and C-BSRs, and the interfaces connecting to the multicast source and user hosts.

Configuring an RP

- An RP must be configured if ASM multicast services need to be provided on a PIM network.
- An RP can be configured in three models: configuring only a static RP, configuring only a dynamic RP, and configuring both a static RP and dynamic RP. If both a static RP and dynamic RP are configured, the dynamic RP takes precedence over the static RP.

- Configuring a static RP: If not specified, a static RP should be configured on each router.
- Configuring a dynamic RP: If not specified, a C-RP and C-BSR should be configured on one or multiple routers.

Enabling SSM

- SSM must be enabled if SSM multicast services need to be provided on a PIM network.
- If not specified, SSM must be enabled on every router.

Verification

Send multicast packets from the multicast source to the groups within the address rang of ASM and SSM, and join user hosts to these groups.

- Check whether the user hosts can successfully receive packets from each group.
- Check whether PIM-SM routing entries are created on routers correctly.

Related Commands

Enabling IPv4 Multicast Routing

Command	**ip multicast-routing**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling PIM-SM

Command	**ip pim sparse-mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports(APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

Enabling PIM-SM Passive

Command	**ip pim sparse-mode passive**
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports(APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

Configuring a Static RP

Command	**ip pim rp-address** *rp-address* [*access_list*]
Parameter Description	*rp-address*: Indicates the address of an RP. *access_list*: Specifies the range of multicast group addresses served by a static RP using an ACL. By default, an RP services all groups.
Command Mode	Global configuration mode
Usage Guide	This command is used to locate a static RP. A static RP should be one with good routing performance. It is recommended that the address of the loopback interface be used as the static RP address. The static RP of all routers must be the same (including the RP address and the range of multicast group addresses it serves). It is recommended that the address of the loopback interface be used as the static RP address. The load can be shared if you configure multiple static RPs to serve different multicast group addresses. It is recommended that the address of the loopback interface be used as the static RP address.

Configuring a C-RP

Command	**ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *seconds*] [**group-list** *access_list*]
Parameter Description	*interface-type interface-number*: Uses the address of this interface as the address of the C-RP. **priority** *priority-value*: Competes for the RP priority. A greater value indicates a higher priority. The value ranges from 0 to 255 (192 by default). **interval** *seconds*: Indicates the interval for sending a C-RP packet to a BSR. The value ranges from 1 to 16,383 (60 by default). **group-list** *access_list*: Specifies the range of multicast group addresses served by a C-RP using an ACL. By default, a C-RP services all multicast groups.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure a router as a C-RP. A C-RP should be one with good routing performance. A C-RP and C-BSR can be on the same router or different routers. It is recommended that the address of the loopback interface be used as the C-RP address. If multiple C-RPs serve the same group, redundancy can be realized.

	If multiple C-RPs serve the different groups, load can be shared.

Configuring a C-BSR

Command	**ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]]
Parameter Description	*interface-type interface-number*: Uses the address of this interface as the address of the C-BSR. *hash-mask-length*: Indicates the length of hash mask used to competing for the RP. The value ranges from 0 to 32 (10 by default). *priority-value*: Indicates the priority for competing for the BSR. A greater value indicates a higher priority. The value ranges from 0 to 255 (64 by default).
Command Mode	Global configuration mode
Usage Guide	This command is used to configure a router as a C-BSR. A C-BSR should be one with good routing performance. A C-RP and C-BSR can be on the same router or different routers. It is recommended that the address of the loopback interface be used as the C-BSR address. Configuring multiple C-BSRs can realize redundancy.

Enabling SSM

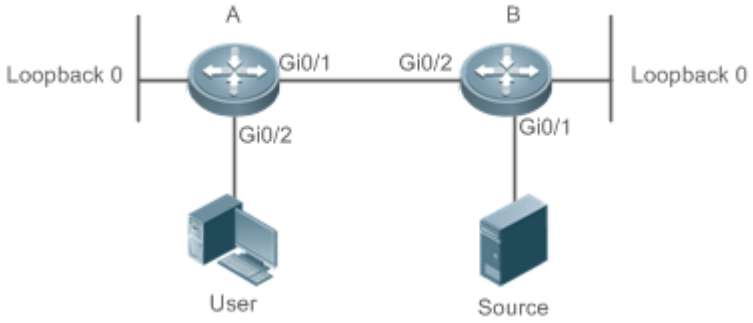
Command	**ip pim ssm** { **default** | **range** *access_list* }
Parameter Description	**default**: Indicates the default range of SSM group addresses, which is 232.0.0.0/8. **range** *access_list*: Specifies the range of SSM group addresses using an ACL.
Command Mode	Global configuration mode
Usage Guide	The SSM group addresses configured on all routers must be the same.

Displaying the PIM-SM Routing Entry

Command	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Parameter Description	*group-or-source-address*: Indicates a multicast group address or source address (the two addresses cannot be multicast group addresses or source addresses at the same time).
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Check whether sufficient routing entries are provided. Check the upstream and downstream interface lists and ensure that a correct SPT tree is created.

Configuration Example

Enabling IPv4 Multicast Routing to Support ASM and SSM

Scenario **Figure 4-4**	
Configuration Steps	● Configure a IPv4 unicast routing protocol (such as OSPF) on a router, and the router is reachable for the unicast route of a loopback interface. (Omitted) ● Enable IPv4 multicast routing on all the routers. ● Enable PIM-SM on all the interconnected interfaces of the routers, Source, and Receiver. ● Configure C-RP and C-BSR on the loopback interfaces of Router A and Router B, and enable PIM-SM on the loopback interfaces. ● Enable SSM on all routers. ● Enable IGMPv3 on the router interfaces connecting to user terminals. (Omitted)
A	A# configure terminal A(config)# ip multicast-routing A(config)# ip pim ssm default A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# interface GigabitEthernet 0/2 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# interface loopback 0 A(config-if)# ip pim sparse-mode A(config-if)# exit A(config)# ip pim rp-candidate loopback 0
B	B# configure terminal B(config)# ip multicast-routing

	B(config)# ip pim ssm default B(config)# interface GigabitEthernet 0/1 B(config-if)# ip pim sparse-mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if)# ip pim sparse-mode B(config-if)# exit B(config)# interface loopback 0 B(config-if)# ip pim sparse-mode B(config-if)# exit B(config)# ip pim bsr-candidate loopback 0
Verification	Send packets from S (192.168.1.10) to G 1 (229.1.1.1) and G2 (232.1.1.1). Add the user to G 1 and G 2, and specify the source when the user joins G 2. ● Check that multicast packets from S (192.168.1.10) to G 1 and G 2 are received by the user. ● Check the PIM-SM routing entries on Router A and Router B. Entries (*, 229.1.1.1), (192.168.1.10, 229.1.1.1), and (192.168.1.10, 232.1.1.1) should be displayed.
A	switch#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 3 (S,G) Entries: 2 (S,G,rpt) Entries: 2 FCR Entries: 0 REG Entries: 0 (*, 229.1.1.1) RP: 192.168.10.10 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

```
Local
0 . . . i . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
FCR:


(192.168.1.10, 229.1.1.1)
RPF nbr: 192.168.2.1
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 207 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Outgoing
0 . . . o . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

```
(192.168.1.10, 229.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  .  o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

(*, 232.1.1.1)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
FCR:
```

```
(192.168.1.10, 232.1.1.1)
RPF nbr: 192.168.2.1
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 207 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  .  o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .


(192.168.1.10, 232.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

	1 . . . . . . Outgoing 0 . . . o . . . . . . 1 . . . . . . (*, 239.255.255.250) RP: 192.168.10.10 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . . i . . . . . . 1 . . . . . . Joined 0 . j . . . . . . 1 . . . . . . Asserted 0 . . . . . . 1 . . . . . . FCR: A#
B	B#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1

```
(192.168.1.10, 229.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 38 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Joined
0  .  .  j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

(192.168.1.10, 229.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

(192.168.1.10, 232.1.1.1)
RPF nbr: 0.0.0.0
```

```
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 38 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Joined
0  .  .  j  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  o  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .

(192.168.1.10, 232.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Pruned
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Outgoing
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
(*, 239.255.255.250)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: JOINED
jt_timer expires in 15 seconds
```

```
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
FCR:
```

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- SSM is not enabled on a router or the SSM group address is different from that of the others'.
- PIM-SM is not enabled on an interface (for example, the interface is configured as a C-RP or C-BSR interface, or is used to connecting to the user host or used as an interface of the multicast source).
- IGMPv3 is not enabled on an interface connecting to the used host.
- RP is not configured on the network.
- A static RP is not configured on a router, or the configured static RP is different from that on other routers.
- C-RPs are configured on the network, but C-BSRs are not.
- Static RPs, C-RPs or C-BSRs are unreachable for unicast routes.

4.4.2 Configuring PIM-SM Neighbors

Configuration Effect

- Coordinate protocol parameters and adjust parameters in the Hello packet.
- A RIM router is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.
- Maintain neighbor relationships and filter the neighbors.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure parameters on PIM router interfaces If not specified.

Verification

Configure the parameters of a Hello packet sent from an interface and run **debug ip pim sparse-mode packet** to display the parameters.

Enable neighbor filtering and run **show ip pim sparse-mode neighbor** to display neighbor information.

Related Commands

Configuring the Interval for Sending Hello Packets

Command	**ip pim query-interval** *interval-seconds*
Parameter Description	Indicates the interval for sending Hello packets, Indicates the suppression time of a register packet in the unit of seconds. The value ranges from 1 to 65,535 (30 by default).
Command Mode	Interface configuration mode
Usage Guide	Every time when the interval for sending Hello packets is updated, the holdtime value is automatically updated as 3.5 times of the interval. If the result of the interval for sending Hello packets multiplied by 3.5 is greater than 65, 535, the holdtime value is forcibly updated as 18,725.

Configuring the Prune Propagation Delay

Command	**ip pim propagation-delay** *milliseconds*
Parameter Description	*milliseconds*: The unit is ms. The value ranges from 1 to 32,767 (500 by default).
Command Mode	Interface configuration mode
Usage Guide	Once the prune propagation delay or prune override interval is changed, the Join/Prune packet override interval will be changed. As specified by the protocol, the Join/Prune packet override interval must be smaller than the holdtime of a Join/Prune packet; otherwise, short break-up of traffic may be caused. The administrator should maintain such configuration.

Configuring the Prune Override Interval

Command	**ip pim override-interval** *milliseconds*
Parameter Description	*milliseconds*: The unit is ms. The value ranges from 1 to 65,535 (2,500 by default).
Command Mode	Interface configuration mode
Usage Guide	Once the prune propagation delay or prune override interval is changed, the Join/Prune packet override interval will be changed.

	As specified by the protocol, the Join/Prune packet override interval must be smaller than the holdtime of a Join/Prune packet; otherwise, short break-up of traffic may be caused. The administrator should maintain such configuration.

Enabling Suppression Capability of an Interface for Sending Join Packets

Command	**ip pim neighbor-tracking**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Once Join packets suppression of an interface is enabled, when the present router is to send a Join packet to the upstream neighbor, which has sent a Join packet to its own upstream neighbor, the present router will not send the Join packet; if Join packets suppression is disabled, the Join packet will be sent. When Join packets suppression from downstream receivers are disabled, upstream neighbors will learn how many downstream neighbors are there by counting the Join packets it received, which is called neighbor tracking.

Configuring the Delay for Sending Hello Packets

Command	**ip pim triggered-hello-delay** *interval-seconds*
Parameter Description	*Seconds*: The unit is second. The value ranges from 1 to 5 (5 by default).
Command Mode	Interface configuration mode
Usage Guide	When a PIM interface is enabled or detects a new neighbor, a triggered-hello-delay packet is used to generate a random time. Within the time, the interface sends Hello packets.

Configuring the DR Priority of a Hello Packet

Command	**ip pim dr-priority** *priority-value*
Parameter Description	*priority-value*: Indicates the priority. A greater value indicates a higher priority. The value ranges from 0 to 4,294,967,294 (1 by default).
Command Mode	Interface configuration mode
Usage Guide	A DR may be selected based on the following principles: If all the Hello packets sent from the routers on a local area network (LAN) are configured with priorities, when selecting a DR, the priorities will be compared, and the router with the highest priority will be selected as the DR. If the priority of all routers is the same, their IP addresses will be compared, and the router with the maximum IP address will be selected as the DR. If the priority of the Hello packets sent from a certain router is not configured, the IP addresses of the routers will be compared, and the router with the maximum IP address will be selected as the DR.

Configuring Neighbor Filtering

Command	**ip pim neighbor-filter** *access_list*
Parameter Description	*access_list*: Configures the range of neighbor addresses using a standard IP ACL. The value can be set from 1 to 99 or a string.
Command Mode	Interface configuration mode
Usage Guide	Enabling neighbor filtering can enhance the security of the PIM network and limit the range of legible neighbor addresses. Once a neighbor is filtered out, PIM-SM will not establish peering with it or stop the peering with it.

Displaying the Neighbor Information of an Interface

Command	**show ip pim sparse-mode neighbor** [**detail**]
Parameter Description	**detail**: Displays detailed information.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure the interval for sending Hello packets as 50s. ● Configure the prune propagation delay as 400 ms. ● Configure the prune override interval as 3,000 ms. ● Enable suppression capability of an interface for sending Join packets. ● Configure the delay for sending Hello packets as 3s. ● Configure the DR priority of a hello packet as 5.
	Ruijie# configure terminal Ruijie (config)#int gi 0/1 Ruijie (config-if-GigabitEthernet 0/1)#ip pim query-interval 50 Ruijie (config-if-GigabitEthernet 0/1)#ip pim propagation-delay 400 Ruijie (config-if-GigabitEthernet 0/1)#ip pim override-interval 3000 Ruijie (config-if-GigabitEthernet 0/1)#ip pim triggered-hello-delay 3 Ruijie (config-if-GigabitEthernet 0/1)#ip pim neighbor-tracking
Verification	Run **debug ip pim sparse-mode packet** to display the parameters of a Hello packet.
	Ruijie# debug ip pim sparse-mode packet

	00:01:49:43: %7: VRF(0): Hello send to GigabitEthernet 0/1 00:01:49:43: %7: Send Hello packet 00:01:49:43: %7: Holdtime: 175 00:01:49:43: %7: T-bit: on 00:01:49:43: %7: Propagation delay: 400 00:01:49:43: %7: Override interval: 3000 00:01:49:43: %7: DR priority: 5 00:01:49:43: %7: Gen ID: 355154648 00:01:49:43: %7: RPF Vector capable
Configuration Steps	Configure neighbor filtering and set the allowed address range to 192.168.1.0 to 192.168.1.255.
	Ruijie# configure terminal Ruijie (config)#int gi 0/1 Ruijie (config-if-GigabitEthernet 0/1)# ip pim neighbor-filter 1 % access-list 1 not exist Ruijie(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Ruijie(config)#
Verification	Display neighbor information before neighbor filtering is configured.
	Ruijie# show ip pim sparse-mode neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode 192.168.36.89 GigabitEthernet 0/1 01:12:13/00:01:32 v2 1 / P
	Display neighbor information after neighbor filtering is configured.
	Ruijie# show ip pim sparse-mode neighbor

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

4.4.3 Configuring BSR Parameters

Configuration Effect

- Configure the address range of BSM packets.

Notes

- Basic PIM-SM functions must be configured.
- C-RPs and C-BSRs must be configured.
- Boarders must be configured on the interfaces between domains.

Configuration Steps

Configuring Boarders

- Boarders must be configures if there are multiple domains.
- Boarders are configured on the interfaces separating two domains.

Configuring BSM Packets Limit on a PIM Router

- Optional.
- If not specified, BSM packets limit can be configured on all PIM routers.

Configuring a C-BSR to Inspect the Address Range of a C-PR

- Optional.
- If not specified, C-PR range inspection can be configured on all C-BSRs.

Allowing a C-BSR to Receive a C-RP-ADV Packet Whose Prefix-Count Is 0

- Optional.
- If not specified, this function can be configured on all C-BSRs.

Verification

Border Inspection

Enable basic PIM-SM functions. Configure two routers to be in different domains, configure Router B as the C-BSR, and Router A to receive BSM packets.

Configure the junction of Router A and Router B as the border so that Router A does not receive BSM packets.

Configuring to Inspect BSM Packets Limit on a PIM Router

When basic PIM-SM functions are enabled, and Router B is set as the C-BSR, Router A can receive BSM packets. When the address range of C-BSRs are limited on Router A, BSM packets will not be received by Router A.

Configuring a C-BSR to Inspect the Address Range of a C-PR

When basic PIM-SM functions are enabled, Router B is set as the C-BSR, and Router A as the C-RP, if the address range of the C-RPs is limited on C-BSR, Router B will not receive the rackets sent from the C-RPs.

Related Commands

Configuring BSR Boarders

Command	**ip pim bsr-border**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To prevent BSM flooding, you can configure a BSR boarder on an interface, so that the BSM packets arriving at this interface will be discarded but not forwarded.

Configuring BSM Packets Limit on a PIM Router

Command	**ip pim accept-bsr list** { <1-99> | <1300-1999> | *WORD* }
Parameter Description	**list** *access-list*: Configures the range of BSR addresses using a standard IP ACL. The value can be 1 to 99, 1,300 to 1,999, or a string.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, PIM-SM routers receive only the BSM packets sent from legible BSRs.

Configuring a C-BSR to Inspect the Address Range of a C-PR

Command	**ip pim accept-crp list** *access-list*
Parameter Description	**list** *access-list*: Specifies the range of C-RP addresses and the multicast group addresses they serve using an extended IP ACL. The value can be 100 to 199, 2,000 to 2,699, or a string.
Command Mode	Global configuration mode
Usage Guide	This command should be configured on a C-BSR. When the C-BSR becomes a BSR, it can set the range of legible C-RP addresses and the range of multicast group addresses they serves.

Displaying BSM Packets Information

Command	**show ip pim sparse-mode bsr-router**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Displaying the Packets of All RPs and the Multicast Group Addresses They Serve

Command	**show ip pim sparse-mode rp mapping**
Parameter Description	N/A

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring BSR Boarders

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● On Router A, configure the address of the C-RP as 192.168.8.8. ● On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ● Configure a BSR boarder on the junction of Router A and Router B.
	Ruijie# configure terminal Ruijie(config)# int GigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# ip pim bsr-border Ruijie(config)# end
Verification	Before configuring the boarder, display the BSM information on Router A.
	Ruijie# show ip pim sparse-mode bsr-router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 192.168.6.6 Uptime: 01:14:25, BSR Priority: 64, Hash mask length: 10 Next bootstrap packet in 00:00:52 Role: Candidate BSR Priority: 64, Hash mask length: 10 State: Elected BSR Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06
	⚠ Candidate RP: Indicates all the C-RPs configured on the existing router. It does not include the C-RPs configured on other routers.
	After the boarder is configured, display the BSM information on Router A.
	Ruijie# show ip pim sparse-mode bsr-router

Configuring BSM Packets Limit on a PIM Router, Filtering BSM Source Addresses, and Configuring the Range of BSM Source Addresses to 192.168.1.1 to 192.168.1.255

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● On Router A, configure the address of the C-RP as 192.168.8.8. ● On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ● On Router A, configure the range of allowed BSM source addresses to 192.168.1.1 to 192.168.1.255.
	Ruijie# configure terminal Ruijie(config)# ip pim accept-bsr list 1 % access-list 1 not exist Ruijie(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Ruijie(config)#
Verification	Before configuring BSM packets limit, display the BSM information on Router A.
	Ruijie#show ip pim sparse-mode bsr-router PIMv2 Bootstrap information BSR address: 192.168.6.6 Uptime: 00:00:11, BSR Priority: 64, Hash mask length: 10 Expires: 00:01:59 Role: Non-candidate BSR Priority: 0, Hash mask length: 10 State: Accept Preferred Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06
	After BSM packets limit is configured, display the BSM information on Router A.
	Ruijie# show ip pim sparse-mode bsr-router Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06

Configuring a C-BSR to Inspect the Address Range of a C-PR, Filtering C-RP Addresses, and Configuring the Range of C-RP Addresses to 192.168.1.1 to 192.168.1.255

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● On Router A, configure the address of the C-RP as 192.168.8.8.

	● On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ● On Router B, configure the range of allowed C-RP source addresses to 192.168.1.1 to 192.168.1.255.
	Ruijie# configure terminal Ruijie(config)# ip pim accept-crp list 100 % access-list 1 not exist Ruijie(config)# access-list 1 permit 192.168.1.0 0.0.0.255 Ruijie(config)#
Verification	Before configuring C-RP filtering, display the information of all RP groups on Router B.
	Ruijie#show ip pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.8.8(Not self) Info source: 192.168.8.8, via bootstrap, priority 192 Uptime: 00:15:16, expires: 00:02:18 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 18:52:30, expires: 00:02:00
	After C-RP filtering is configured, display the information of all RP groups on Router B.
	Ruijie#show ip pim sparse-mode rp mapping PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 21:38:20, expires: 00:02:10
	⚠ After C-RP filtering is configured on a router, only the C-RP packets sent from other routers are filtered, and those sent from the present router are not filtered.

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

- C-BSRs are not configured.
- The BSR border is not configured on the interfaces of different domains.

4.4.4 Configuring RP and DR Parameters

Configuration Effect

- Ignore the C-RP priority and reselect an RP.
- Detect the reachability of an RP for the source DR.
- Configure the range of (S, G) addresses of source register packets, and allow the ASM to serve only the multicast packets within the range.
- Limit the speed of the source DR for sending register packets.
- Configure the checksum of the register packet length.
- Configure an RP to decapsulate register packets and forward the multicast packets to downstream interfaces.
- Configure the source IP address of a register packet.
- Configure the suppression time of a register packet.
- Configure the inspection time of a null register packet.
- Configure the (S, G) lifetime based on the register packet received by an RP.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

↘ **Ignoring the C-RP Priority and Reselecting an RP**

- Optional.
- If not specified, the C-RP priority can be disabled on every router.

↘ **Detecting the Reachability of an RP for the Source DR**

- Optional.
- If not specified, this function can be enabled on the DR connected directly to the data source.

↘ **Configuring the Range of Source Register (S, G) Addresses**

- Optional.
- If not specified, source register address filtering can be enabled on all C-RPs or static RPs.

↘ **Limiting the Speed of the Source DR for Sending Register Packets**

- Optional.

- If not specified, this function can be enabled on the source DR.

Configuring the Checksum of the Register Packet Length

- Optional.
- If not specified, this function can be enabled on all C-RPs or static RPs.

Configuring Whether to Forward the Multicast Packet After Decapsulating a Register Packet

- Optional.
- If not specified, this function can be enabled on all C-RPs or static RPs.

Configuring the Source IP Address of a Register Packet

- Optional.
- If not specified, the source IP address of a register packet can be configured on the DR connected directly to the data source.

Configuring the Suppression Time of a Register Packet

- Optional.
- If not specified, the suppression time of a register packet can be configured on the DR connected directly to the data source.

Configuring the Inspection Time of a Null Register Packet

- Optional.
- If not specified, the inspection time of a null register packet can be configured on the DR connected directly to the data source.

Configuring the (S, G) Lifetime Based on the Register Packet Received by an RP

- Optional.
- If not specified, the (S, G) lifetime can be configured on all C-RPs or static RPs.

Verification

Ignoring the C-RP priority

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the C-RP address as 192.168.5.5, priority as 200, and C-BSR address as 192.168.6.6.

- Run **show ip pim sparse-mode rp** 233.3.3.3 to display the RPs of the present group.

Enabling the Source DR to Detect RP Reachability

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the C-RP address as 192.168.5.5, priority as 192, and C-BSR address as 192.168.6.6. Enable Router B to detect RP reachability.

- Run **show running-config** to check whether the preceding configurations take effect.

Configuring the Range of Source Register (S, G) Addresses

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the address of the C-BSR as 192.168.6.6. Configure the source address a 192.168.1.100 and the multicast group address as 233.3.3.3. On Router A, configure the range of allowed source multicast group addresses to 192.168.2.0 to 192.168.2.255.

- Run **show ip pim sparse-mode mroute** to display the (S, G) entry.

Limiting the Speed of the Source DR for Sending Register Packets

Configure the speed of Router B for sending register packets, and run **show ip pim sparse-mode track** to display the number of packets that has been sent.

Configuring the Checksum of the Register Packet Length

On Router A, configure to calculate the checksum of the entire register packet length but not just the packet header. Run **show running-config** to check the configuration.

Forwarding an RP Register Packet After It Is Decapsulated

On Router A, configure to forward a register packet after it is decapsulated. Run **show running-config** to display the configuration.

Configuring the Source IP Address of a Register Packet

Configure the source address of a register packet on Router B, and run **show running-config** to display the configuration.

Configuring the Suppression Time of a Register Packet and the Inspection Time of a Null Register Packet

On Router B, configure the suppression time and inspection time of a register packet, and run **show ip pim sparse-mode track** to display the configuration.

Configuring an RP to Receive Register Packets and the (S, G) Lifetime

On Router A, configuring an RP to receive register packets and the (S, G) lifetime, and run **show ip pim sparse-mode mroute** to display the maximum (S, G) lifetime.

Related Commands

Ignoring the C-RP priority

Command	**ip pim ignore-rp-set-priority**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Displaying the RP Corresponding to a Group

Command	**show ip pim sparse-mode rp-hash** *group-address*
Parameter Description	*group-address*: Indicates the parsed multicast group address.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Enabling the Source DR to Detect RP Reachability

Command	**ip pim register-rp-reachability**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, the source DR will detect the RP reachability before sending a register packet. If the RP is unreachable, the packet will not be sent.

Configuring the Range of Source Register (S, G) Addresses

Command	**ip pim accept-register** { **list** *access-list* [**route-map** *map-name*] | **route-map** *map-name* [**list** *access-list*] }
Parameter Description	**list** *access-list*: Configures the range of (S, G) addresses using an extended IP ACL. The value can be 100 to 199, 2,000 to 2699, or a string. **route-map** *map-name*: Configures the range of (S, G) addresses using a route map.
Command Mode	Global configuration mode
Usage Guide	This command is run on a static RP or a C-RP to specify the source address and multicast group address of a register packet.

Displaying a Multicast Routing Entry

Command	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Parameter Description	*group-or-source-address*: Indicates a multicast group address or source address (the two addresses cannot be multicast group addresses or source addresses at the same time). **Proxy:** Indicates the RPF vector carried by an entry.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	You can specify either a multicast group address or source address, or both a multicast group address and source address; or you can specify neither a multicast group address nor source address. The two addresses cannot be multicast group addresses or source addresses at the same time.

Limiting the Speed of the Source DR for Sending Register Packets

Command	**ip pim register-rate-limit** *rate*
Parameter Description	*Rate*: Indicates the maximum number of register packets that can be sent each second. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	This command takes effect for only the register packet of each (S, G) packet, but not all the register packets in the entire system. Enabling this command can reduce the burden on the source DR and RPs. Only the packets within the speed limit can be sent.

Displaying the Counters of PIM-SM Packets

Command	**show ip pim sparse-mode track**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	The start time for counting PIM-SM packets is automatically enabled upon system startup. Run **clear ip pim sparse-mode track** to reset the start time and clear the PIM-SM packet counters.

Calculating the Checksum of the Entire Register Packet Length

Command	**ip pim register-checksum-wholepkt** [**group-list** *access-list*]
Parameter Description	**group-list** *access-list*: Configures the multicast group addresses applicable to this configuration using an ACL. access-list: The value can be set to 1 to 99, and 1300 to 1999. It also supports the naming of the ACL.
Command Mode	Global configuration mode
Usage Guide	You can enable this function if you want to calculate the length of the entire PIM-SM packet, including that of the multicast packet encapsulated in the register packet, but not just the length of the PIM-SM packet header. If **group-list** *access-list* is specified, this configuration takes effect for all multicast group addresses.

Enabling an RP to Decapsulate a Register Packet and Forward the Multicast Packet to Interfaces

Command	**ip pim register-decapsulate-forward**
Parameter Description	N/A
Command	Global configuration mode

Mode	
Usage Guide	This command is configured on a static RP or a C-RP. It is used to decapsulate a register packet with multicast packet and forward the multicast packet to interfaces. If there are too many register packets to be decapsulated, the CPU will be greatly burdened. In this case, this function is recommended to be disabled.

Configuring the Source IP Address of a Register Packet

Command	**ip pim register-source** { *local_address* | *Interface-type interface-number* }
Parameter Description	*local_address*: Specifies the source IP address of a register packet. *interface-type interface-number*: Specifies the IP address of this interface as the source IP address of the register packet.
Command Mode	Global configuration mode
Usage Guide	The specified address must be reachable. When an RP sends a Register-Stop packet, the PIM router corresponds to this address need to respond. Therefore, it is recommended that a loopback address (or other physical addresses) be used. This configuration does not require the enabling of PIM.

Configuring the Suppression Time of a Register Packet

Command	**ip pim register-suppression** *seconds*
Parameter Description	*Seconds*: Indicates the suppression time of a register packet in the unit of seconds. The value ranges from 1 to 65,535 (60 by default).
Command Mode	Global configuration mode
Usage Guide	If you configure this parameter on a DR, the suppression time of a register packet sent from the DR will be changed. If **ip pim rp-register-kat** is not configured and if you configure this parameter on an RP, the RP keepalive will be changed.

Configuring the Inspection Time of a Null Register Packet

Command	**ip pim probe-interval** *seconds*
Parameter Description	*Seconds*: Indicates the inspection time of a null register packet in the unit of seconds. The value ranges from 1 to 65,535 (5 by default).
Command Mode	Global configuration mode
Usage Guide	The inspection time of a null register packet indicates the period of time for sending a null register packet to an RP before the timeout of suppression time. The inspection time cannot exceed half of the suppression time; otherwise, the configuration will not take effect, and a warning message will be displayed. Meanwhile, the result of suppression time multiplied by 3

	plus the inspection time cannot exceed 65,535, otherwise, a warning will be displayed.

Configuring the Interval of KATs on an RP

Command	**ip pim rp-register-kat** *seconds*
Parameter Description	*Seconds*: Indicates the interval of a KAT in the unit of second. The value ranges from 1 to 65,535 (210 by default).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the RPs of Corresponding Multicast Group Addresses When the C-RP Priority is Considered or Not Considered

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● On Router A, configure the address of the C-RP as 192.168.8.8. ● On Router B, configure the address of the C-RP as 192.168.5.5, priority as 200, and the address of the C-BSR as 192.168.6.6. ● Display the group corresponding to 233.3.3.3. ● Configure to ignore the C-RP priority on Router B.
	`Ruijie# configure terminal` `Ruijie(config)# ip pim ignore-rp-set-priority`
Verification	Display the information before you configure to ignore the C-RP priority.
	`Ruijie# show ip pim sparse-mode rp-hash 233.3.3.3` `RP: 192.168.8.8` `Info source: 192.168.8.8, via bootstrap` `PIMv2 Hash Value 10(mask 255.192.0.0)` `RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102` `RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709`
	Display the information after you configure to ignore the C-RP priority.
	`Ruijie# show ip pim sparse-mode rp-hash 233.3.3.3` `RP: 192.168.5.5` `Info source: 192.168.6.6, via bootstrap`

	PIMv2 Hash Value 10(mask 255.192.0.0) RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102 RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709

Configuring to Inspect the Reachability of a Source RP

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure to inspect the reachability of a source RP.
	Ruijie(config)# ip pim register-rp-reachability
Verification	Run **show running-config** to check whether the following information is displayed.
	Ruijie(config)#show running-config ip pim register-rp-reachability

Configuring the Range of Source Register (S, G) Addresses

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure source address filtering on Router A. The allowed address range is from 192.168.2.0 to 192.168.2.255.
	Ruijie#show ip pim sparse-mode mroute Ruijie(config)#ip pim accept-register list 101 % access-list 101 not exist Ruijie(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 any Ruijie#show ip pim sparse-mode mroute
Verification	Before enabling source address filtering, run **show ip pim sparse-mode mroute** to display the multicast entry, and check whether the (S, G) entry and (S, G, RPT) entry exist.
	Ruijie#show ip pim sparse-mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0

```
REG Entries: 0


(192.168.1.100, 233.3.3.3)
RPF nbr: 192.168.36.90
RPF idx: VLAN 1
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 187 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
     .
Joined
0 . . . . . .
     .
Asserted
0 . . . . . .
     .
Outgoing
0 . . . . . .
     .


(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
     .
Pruned
0 . . . . . .
```

	`.` `Outgoing` `0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .` `.` `(*, 239.255.255.250)` `RP: 192.168.8.8` `RPF nbr: 0.0.0.0` `RPF idx: None` `Upstream State: JOINED` `00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31` `Local` `0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .` `.` `Joined` `0 .` `j . . . . . . . . . . . . . . . . . . . . . . . . . . . . .` `.` `Asserted` `0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .` `.` `FCR:`
	After source address filtering is enabled, run **show ip pim sparse-mode mroute** to display the multicast entry, and check whether the (S, G) entry and (S, G, RPT) entry exist.
	`Ruijie#show ip pim sparse-mode mroute` `IP Multicast Routing Table` `(*,*,RP) Entries: 0` `(*,G) Entries: 1` `(S,G) Entries: 0` `(S,G,rpt) Entries: 0` `FCR Entries: 0`

```
REG Entries: 0


(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
     .
Joined
0 .
    j . . . . . .
    .
Asserted
0 . . . . . .
     .
FCR:
```

Limiting the Speed of the Source DR for Sending Register Packets

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Check the number of PIM-SM packets sent by Router B. ● Check the number of PIM-SM packets sent by Router B in 1s. ● Configure the speed of Router B for sending register packets. ● Check the number of PIM-SM packets sent by Router B in 1s.
	`Ruijie (config)#ip pim register-rate-limit 1`
Verification	Display the number of PIM-SM packets sent by Router B before you configure the speed. The information should be displayed as follows:
	`Ruijie#show ip pim sparse-mode track` `PIM packet counters track` `Elapsed time since counters cleared: 04d01h01m`

```
                    received                    sent
Valid PIM packets:     18754                      29771
Hello:                 11149                      17842
Join-Prune:            0                          3234
Register:              0                          3211
Register-Stop:         3192                       0
Assert:                0                          0
BSM:                   0                          5484
C-RP-ADV:              4413                       0
PIMDM-Graft:           0
PIMDM-Graft-Ack:       0
PIMDM-State-Refresh:   0
Unknown PIM Type:      0


Errors:
Malformed packets:                          0
Bad checksums:                              0
Send errors:                                0
Packets received with unknown PIM version: 0
Ruijie#
```

Display the number of PIM-SM packets sent by Router B in 1s before the speed is configured. The information should be displayed as follows:

```
Ruijie #show ip pim sparse-mode track
PIM packet counters track
Elapsed time since counters cleared: 04d01h04ms


                    received                    sent
Valid PIM packets:     18765                      29789
Hello:                 11154                      17852
Join-Prune:            0                          3236
Register:              0                          3214
Register-Stop:         3195                       0
```

```
Assert:                0                          0
BSM:                   0                          5487
C-RP-ADV:              4416                       0
PIMDM-Graft:           0
PIMDM-Graft-Ack:       0
PIMDM-State-Refresh:   0
Unknown PIM Type:      0


Errors:
Malformed packets:                          0
Bad checksums:                              0
Send errors:                                0
Packets received with unknown PIM version: 0
Ruijie#
```

Display the number of PIM-SM packets sent by Router B after the speed is configured. The information should be displayed as follows:

```
Ruijie#show ip pim sparse-mode track
PIM packet counters track
Elapsed time since counters cleared: 04d01h06m


                    received                    sent
Valid PIM packets:     18777                      29808
Hello:                 11159                      17862
Join-Prune:            0                          3239
Register:              0                          3215
Register-Stop:         3196                       0
Assert:                0                          0
BSM:                   0                          5489
C-RP-ADV:              4419                       0
PIMDM-Graft:           0
PIMDM-Graft-Ack:       0
PIMDM-State-Refresh:   0
```

```
Unknown PIM Type:      0


Errors:
Malformed packets:                          0
Bad checksums:                              0
Send errors:                                0
Packets received with unknown PIM version: 0
Ruijie#
```

Configuring the Checksum of the Register Packet Length

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Calculate the checksum of the entire register packet length. ● Run **show running-config** to check whether the preceding configurations take effect.
	`Ruijie(config)#ip pim register-checksum-wholepkt`
Verification	Display the configurations on Router A, which should be as follows:
	`Ruijie#show running-config` `...` `!` `ip pim register-checksum-wholepkt` `ip pim rp-candidate Loopback 0` `!` `...`

Enabling an RP to Decapsulate a Register Packet and Forward the Multicast Packet to Interfaces

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Enable Router A to forward a register packet. ● Run **show running-config** to check whether the preceding configurations take effect.
	`Ruijie(config)#ip pim register-decapsulate-forward`
Verification	Display the configurations on Router A, which should be as follows:
	`Ruijie#show running-config` `...` `!`

```
!
ip pim register-decapsulate-forward
ip pim register-checksum-wholepkt
ip pim rp-candidate Loopback 0
!
!
!
...
```

Configuring the Source IP Address of a Register Packet

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure the source address of Loop 2 as 192.168.2.2. ● Configure source address interface for the register packet of Router B as Loop 2. ● Run **show running-config** to check whether the preceding configurations take effect.
Verification	Display the configurations on Router B, which should be as follows:

```
Ruijie#show running-config
!
!
!
ip pim register-source Loopback 1
ip pim bsr-candidate Loopback 0
!
!
!
!
```

Configuring the Suppression Time of a Register Packet and the Inspection Time of a Null Register Packet

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure the suppression time of a register packet on Router B to 20s. ● Configure the inspection time of a null register packet on Router B to 2s. ● Run **show ip pim sparse-mode track** to display number of register packets.

```
Ruijie(config)#ip pim register-suppression 20
```

	Ruijie(config)#ip pim probe-interval 2
Verification	Display the number of register packets on Router B. The information should be displayed as follows:
	Ruijie#show ip pim sparse-mode track PIM packet counters track Elapsed time since counters cleared: 04d23h15m received sent Valid PIM packets: 23788 43249 Hello: 13817 23178 Join-Prune: 0 4568 Register: 0 8684 Register-Stop: 4223 0 Assert: 0 0 BSM: 0 6819 C-RP-ADV: 5748 0 PIMDM-Graft: 0 PIMDM-Graft-Ack: 0 PIMDM-State-Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 Ruijie# Ruijie#
	In 18s, display the number of register packets on Router B. The information should be displayed as follows:
	Ruijie#show ip pim sparse-mode track PIM packet counters track

```
Elapsed time since counters cleared: 04d23h17m


                    received                    sent
Valid PIM packets:     23798                      43263
Hello:                 13820                      23184
Join-Prune:            0                          4569
Register:              0                          8685
Register-Stop:         4224                       0
Assert:                0                          0
BSM:                   0                          6820
C-RP-ADV:              5749                       0
PIMDM-Graft:           0
PIMDM-Graft-Ack:       0
PIMDM-State-Refresh:   0
Unknown PIM Type:      0


Errors:
Malformed packets:                          0
Bad checksums:                              0
Send errors:                                0
Packets received with unknown PIM version: 0
Ruijie#
```

Configuring an RP to Receive Register Packets and the (S, G) Lifetime

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure Router A to receive register packets and the (S, G) lifetime is 60s. ● Run **show ip pim sparse-mode mrout** to display number of register packets.
	`Ruijie(config)#ip pim rp-register-kat 60`
Verification	After the lifetime is configured, check that the (S, G) lifetime on Router A does not exceed 60s.
	`Ruijie(config)#show ip pim sparse-mode mroute` `IP Multicast Routing Table`

```
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0


(192.168.1.100, 233.3.3.3)
RPF nbr: 192.168.36.90
RPF idx: VLAN 1
SPT bit: 0
Upstream State: NOT JOINED
kat expires in 49 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
     .
Joined
0 . . . . . .
     .
Asserted
0 . . . . . .
     .
Outgoing
0 . . . . . .
     .


(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
```

```
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
      .
Pruned
0 . . . . . .
      .
Outgoing
0 . . . . . .
      .


(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
      .
Joined
0 .
    j . . . . . .
    .
Asserted
0 . . . . . .
      .
FCR:


Ruijie(config)#
Ruijie(config)#show ip pi
```

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

- The (S, G) of register packets is not configured on a C-RP or static RP, or the configuration is not successful.
- The ACL for limiting the (S, G) of register packets is not configured or the range of (S, G) in this ACL is not correctly configured.
- The range of (S, G) of register packets on each C-RP or static RP is not the same.

4.4.5 Configuring the Interval for Sending a Join/Prune Packet

Configuration Effect

- Change the interval for sending a Join/Prune packet to form an RPT or SPT.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure the interval for sending a Join/Prune packet.

Verification

On Router B, configure the interval for sending a Join/Prune packet as 120s. Run **show ip pim sparse-mode mroute** to display the lifetime of the entry.

Related Commands

↘ **Configuring the Interval for Sending a Join/Prune Packet**

Command	**ip pim jp-timer** *seconds*
Parameter Description	**vrf** *vid*: Specifies VRF. *Seconds*: Indicates the interval for sending a Join/Prune packet. The unit is second. The value ranges from 1 to 65,535 (60 by default).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ **Configuring the Interval for Sending a Join/Prune Packet**

Configuration Steps	• Configure basic PIM-SM functions. (Omitted) • Configure the interval for sending a Join/Prune packet.
	`Ruijie(config)#ip pim jp-timer 120`
Verification	Run **show ip pim sparse-mode mroute** to display the maximum timeout time of a Join/Prune packet.

```
Ruijie(config)#show ip pim sparse-mode mroute
IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 1

(192.168.1.100, 233.3.3.3)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 96 seconds
kat expires in 92 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
     .
1 . . . . . .
     .
Joined
0 . . . . . .
     .
1 . . . . . .
     .
Asserted
0 . . . . . .
     .
1 . . . . . .
     .
Outgoing
```

```
0 . . . . . .
    .
1 . . o . . . . . .
    .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: RPT NOT JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0 . . . . . .
    .
1 . . . . . .
    .
Pruned
0 . . . . . .
    .
1 . . . . . .
    .
Outgoing
0 . . . . . .
    .
1 . . . . . .
    .

(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: JOINED
jt_timer expires in 119 seconds
```

```
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Local
0  .  .  .  .
     i  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
       .
Joined
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
       .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
       .
Asserted
0  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
       .
1  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
       .
FCR:


VSU(config)#
```

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

4.4.6 Configuring the Router of Last Hop to Switch from an RPT to SPT

Configuration Effect

- Switch from an RPT to SPT

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure the router of last hop to switch from an RPT to SPT.

Verification

Configure basic PIM-SM functions first. Configure the source DR to sends the data traffic (*, 233.3.3.3), and the receiving end to join group 233.3.3.3 forcibly to form an RPT. Configure the receiver DR to switch from the RPT to SPT forcibly. Run **show running-config** to display the result.

Related Commands

Enabling SPT switchover

Command	**ip pim spt-threshold** [**group-list** *access-list*]
Parameter Description	**group-list** *access-list*: Specifies the range of multicast group addresses allowed for SPT switchover using an ACL. access-list: The supported value ranges from 1 to 99 or 1,300 to 1,999. Naming an ACL is also supported.
Command Mode	Global configuration mode
Usage Guide	If **group-list** *access-list* is not specified, all groups are allowed to perform SPT switchover.

Configuration Example

Configuring the Router of Last Hop to Switch from an RPT to SPT

Configuration Steps	● Configure basic PIM-SM functions. (Omitted) ● Configure the source DR to send the data traffic of group 233.3.3.3. ● Configure the receiver DR to receive the data traffic of group 233.3.3.3. ● Configure the receiver DR of last hop to switch from an RPT to SPT.
	`Ruijie(config)#ip pim spt-threshold`
Verification	Run **show running-config** to display the configuration.
	`!` `!` `ip pim jp-timer 120` `ip pim spt-threshold` `ip pim rp-candidate Loopback 0` `!` `!` `!`

4.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears multicast routing entries.	**clear ip mroute** { * | *group-address* [*source-address*] }
Clears the counters of multicast routes.	**clear ip mroute statistics** {* | *group-address* [*source-address*] }
Clears the information about dynamic RPs.	**clear ip pim sparse-mode bsr rp-set ***
Clears the counters of PIM-SM packets.	**clear ip pim sparse-mode track**

Displaying

Description	Command
Displays the details of BSR information.	**show ip pim sparse-mode bsr-router**
Displays the PIM-SM information of an interface.	**show ip pim sparse-mode interface** [*interface-type interface-number*] [**detail**]
Displays the local IGMP information about a PIM-SM interface.	**show ip pim sparse-mode local-members** [*interface-type interface-number*]
Displays the information about a PIM-SM multicast routing entry, and displays the RPF vector of a PIM-SM entry using **proxy**.	**show ip pim sparse-mode mroute** [*group-or-source-address* [*group-or-source-address*]]
Displays the information about PIM-SM neighbors.	**show ip pim sparse-mode neighbor** [**detail**]
Displays the information about the next hop of PIM-SM obtained from the NSM.	**show ip pim sparse-mode nexthop**
Displays the information about the RP corresponding the multicast group address *group-address*.	**show ip pim sparse-mode rp-hash** *group-address*
Displays the information about all the RPs and the groups they serve.	**show ip pim sparse-mode rp mapping**

Description	Command
Displays the number of PIM-SM packets sent and received since the statistic start time.	**show ip pim sparse-mode track**

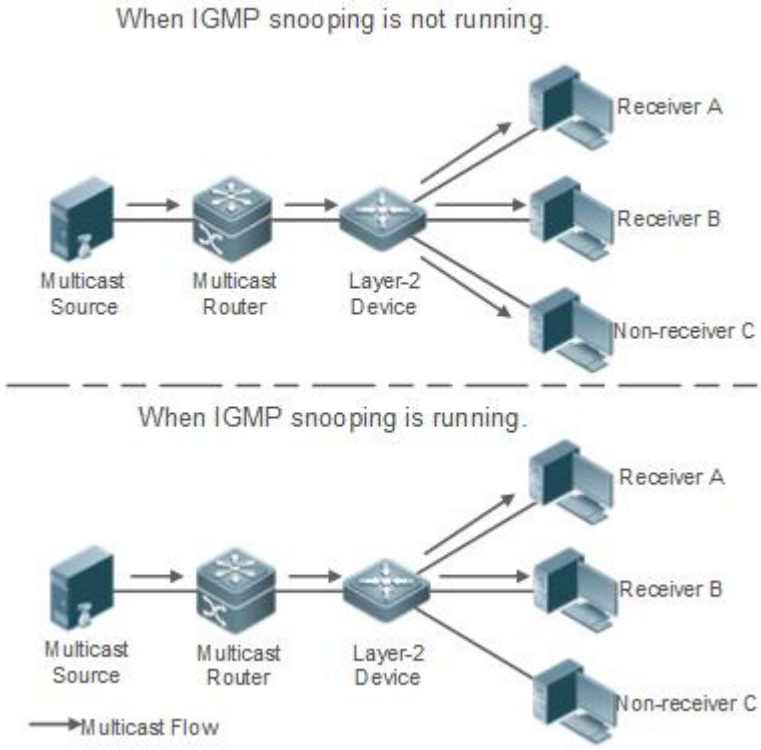
5 Configuring IGMP Snooping

5.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

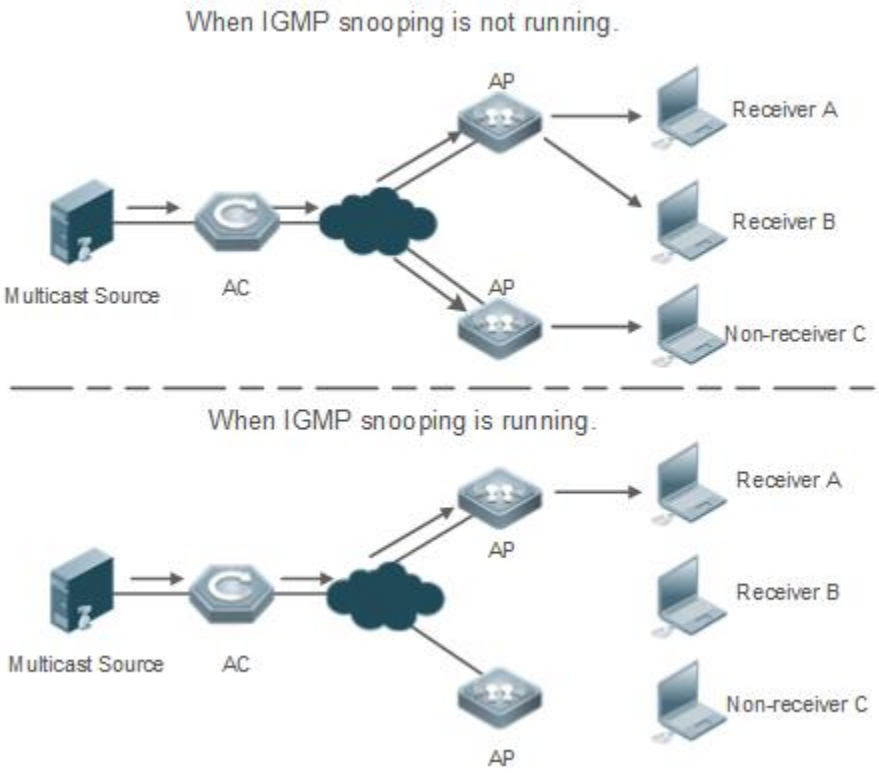
As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 5-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



As shown in the following figure, when IGMP Snooping does not run on the AC and AP in wireless multicast environment, multicast packets are broadcasted within the VLAN of the AC and are broadcasted by the AP to all wireless ports. When IGMP Snooping runs on both the AC and AP, multicast packets of a known multicast profile are not broadcasted but forwarded to specific receivers.

Figure 5-2 Forwarding of IP Multicast Streams in a VLAN Before and After IGMP Snooping Is Enabled on the AC and AP



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

5.2 Applications

Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Shared Multicast Services (Multicast VLAN)	Multiple users can share the multicast traffic of the same VLAN.
Premium Channels and Preview	Controls the range of multicast addresses that allow user demanding and allows preview for profiles who are inhibited from demanding.
Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.

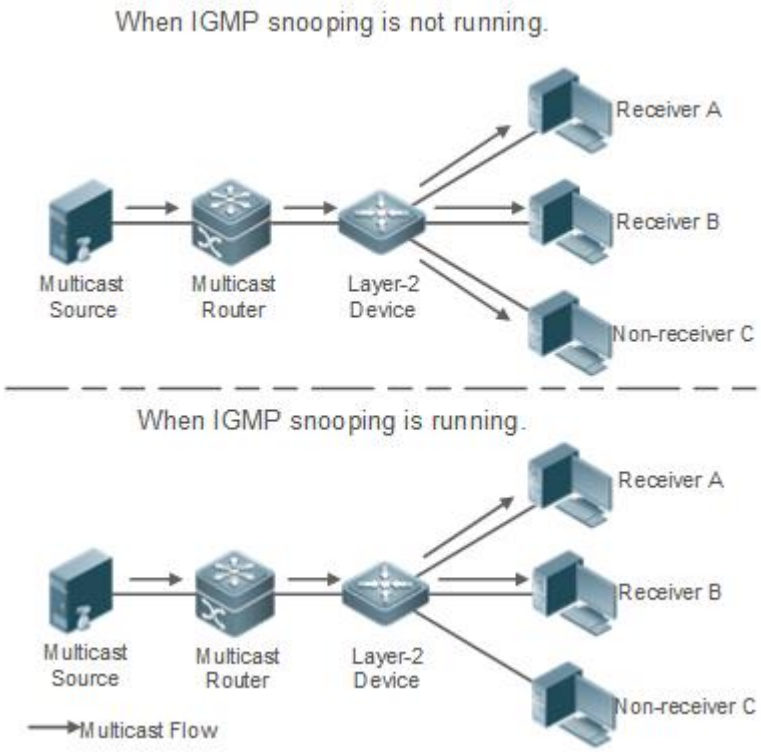
5.2.1 Layer-2 Multicast Control

Scenario

- As shown in the following figure, multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to

all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcast within the VLAN but transmitted to designated receivers.

Figure 5-3 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



Deployment

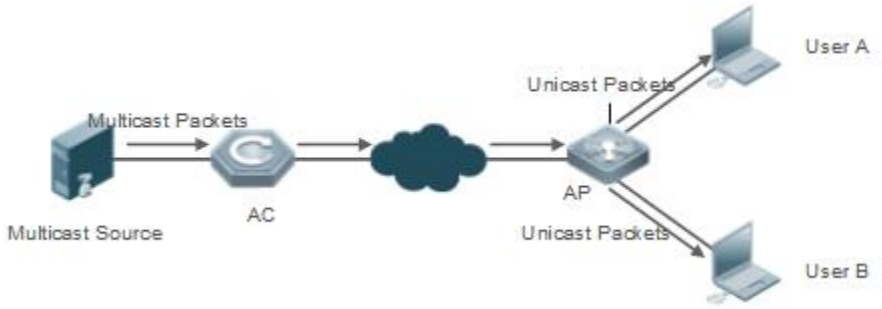
- Configure basic IGMP snooping functions.
-

5.2.2 Multicast-to-Unicast Conversion

Scenario

- When multicast-to-unicast conversion is not configured, packets are transmitted from the AP to STAs in multicast mode. There is no acknowledgement and retransmission mechanism for multicast packets in wireless networks. As a result, severe packet loss occurs, which affect experience of wireless multicast services in video on demand and other applications. Wireless multicast packets between the AP and STAs can be configured to be transmitted in multicast-to-unicast conversion mode in order to reduce the packet loss rate and enhance user experience.

Figure 5-4 Multicast-to-Unicast Conversion



Deployment

- Configure the multicast-to-unicast conversion function.

The function is available only in wireless multicast scenarios.

5.3 Features

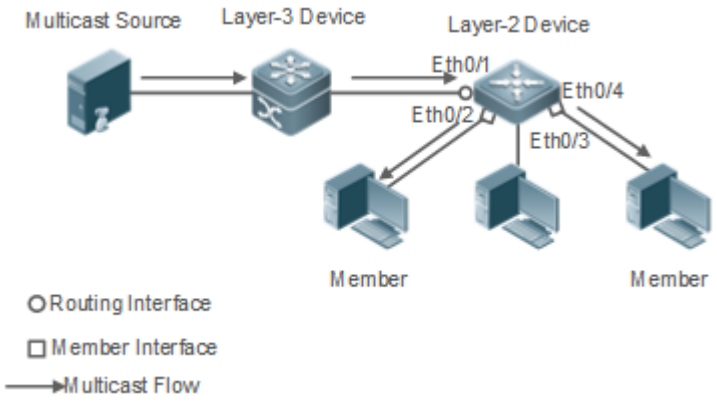
Basic Concepts

Multicast Router Ports and Member Ports

IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 5-5 Networking Topology of Two IGMP Snooping Ports

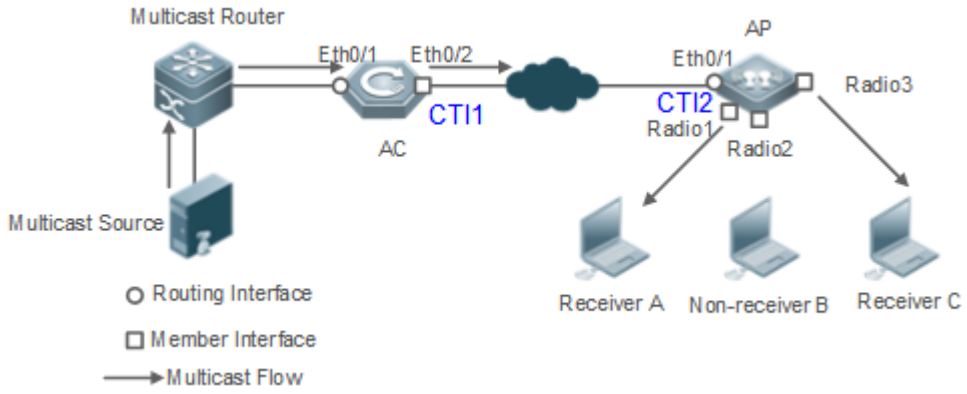


- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device

can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.

- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.
- Wireless devices have wireless ports in comparison with common wired devices, and the communication between an AC and APs is made by establishing CAPWAP tunnels. After a CAPWAP tunnel is established between an AC and an AP, CTI1 and CTI2 interfaces are respectively virtualized on the AC and AP for communication. The following figure shows multicast router ports and member ports on the AC and AP.

Figure 5-6 Two Types of Ports in Wireless Environment



- Multicast router port: When the AC receives the PIM Hello or IGMP Query packet from the upstream multicast router (Layer-3 multicast device), the multicast router port Ethq/1 forms. When the AP receives the PIM Hello or IGMP Query packet forwarded by the AC, the multicast router port CTI2 also forms.
- Member port: also called listener port, that is, the port on a device for connecting to a multicast member. When Ports Radio1 and Radio3 on the AP receive Report packets from a wireless user receiver, they learn the wireless port as a member port. When the virtual interface CTI1 receives Report packets forwarded by the AP, it also learns the relevant wireless port as a member port.

IGMP Snooping Forwarding Entry

The device running IGMP snooping forwards IP multicast packets in accordance with the IGMP snooping forwarding entry.

An IGMP snooping forwarding entry includes the following items: source address (S), profile address (G), VLAN ID (VLAN_ID), multicast router port, and member port. It indicates that packets of required features (including S, G, and VLAN_ID) should enter the multicast router port and exit from a member port. An IGMP snooping forwarding entry is identified using a group of S, G, and VLAN_ID.

To display the IGMP snooping forwarding entry, run the **show ip igmp snooping gda-table** command.

```
Ruijie# show ip igmp snooping gda-table

Multicast Switching Cache Table
```

```
  D: DYNAMIC  //Dynamic member port
  S: STATIC   //Static member port
  M: MROUTE   //Multicast router port (dynamic or static)
(*, 233.3.6.29, 1):   //(S: any; G: 233.3.6.29; VLAN_ID: VLAN 1)
  VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
    caPWAP-Tunnel 0/1(D)   // CAPWAP tunnel
(*, 233.3.6.30, 1):   //S: any; G: 233.3.6.30; VLAN_ID: VLAN 1)
  VLAN(1) 2 OPORTS:
GigabitEthernet 0/2(M)
GigabitEthernet 0/1(D)


(*,239.1.1.1, 1):  //(any source address, with the group address of 239.1.1.1 and VLAN ID of 1)
VLAN(1) 1 OPORTS:
    dot11radio 1/0.1 (D)  //wireless interface
```

Overview

Feature	Description
Listening to IGMP Packets	Discovers and identifies the router port and member port to establish and maintain the IGMP snooping forwarding entries. :
IGMP Snooping Working Modes	Provides independent or shared multicast services to the user VLAN.
Multicast Security Control	Controls the multicast service scope and load to prevent illegal multicast traffic.
Profile	Defines the range of multicast addresses that permit or deny user requests for reference of other functions.
Handling QinQ	Sets the forwarding mode of multicast packets on the QinQ interface.
IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.
Configuring Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.

Optimizing Multicast Wireless Environment Configuration	Ignores port timer resetting for query packets.

5.3.1 Listening to IGMP Packets

A device running IGMP snooping analyzes IGMP packets received, and finds and identifies the router port and member port using these packets, thereby creating and maintaining an IGMP snooping entry.

Working Principle

A device running IGMP snooping can identify and handle the following types of IGMP packets:

Query Packets

An IGMP querier periodically sends General Query packets. When the IGMP querier receives Leave packets, it sends Group-Specific Query packets.

When the device running IGMP snooping receives the Query packets, it performs the following operations within the VLAN:

- Forward the IGMP Query packets to all the ports (except the receiving port of these packets).
- If the receiving port is a dynamic router port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If the receiving port is not a dynamic router port, use it as a dynamic router port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

Report Packets

When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.

By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets. For IGMPv3 Report packets, it processes profile information but does not process carried source information. IGMP Snooping v3 can be configured to process all information in IGMPv1, IGMPv2, and IGMPv3 packets.

When the device running IGMP snooping receives the Report packets, it performs the following operations within the VLAN:

- Forward the Report packets from all the router ports. After the **ip igmp snooping suppression enable** command is run in one IGMP query cycle, only the first report received by each profile will be forwarded.
- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

Leave Packets

If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

Configuring the Aging Time of a Dynamic Router Port

The default aging time is 300s.

When a dynamic router port receives a query packet, the aging timer of the port is enabled or reset.

Run **ip igmp snooping dyn-mr-aging-time** to configure the aging time of the dynamic router port.

Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

Configuring the IGMP Snooping Version

The default version is IGMP Snooping v2, which processes only IGMPv1 and IGMPv2 packets. It conducts simple processing on IGMPv3 packets and does not process source information carried in packets.

Run the **ip igmp snooping version 3** command to configure IGMP Snooping v3 to process all information in IGMPv3 packets.

Run the **no ip igmp snooping version** command to restore IGMP Snooping v2.

5.3.2 IGMP Snooping Working Modes

A device running in the three modes (IVGL, SVGL, and IVGL-SVGL) of IGMP snooping can provide independent multicast services or shared multicast services to the user VLAN.

Working Principle

IVGL

In IVGL mode, a device running IGMP snooping can provide independent multicast services to each user VLAN.

Independent multicast services indicate that multicast traffic can be forwarded only within the VLAN it belongs to, and a user host can subscribe to the multicast traffic within the VLAN that the host belongs to.

SVGL

In SVGL mode, a device running IGMP snooping can provide shared multicast services to the user VLAN.

Shared multicast services can be provided only on shared VLANs and sub VLANs and SVGL multicast addresses are used. In a shared VLAN, the multicast traffic within the range of SVGL multicast addresses is forwarded to a sub VLAN, and the user hosts within the sub VLAN subscribe to such multicast traffic from the shared VLAN.

- In a shared VLAN and sub VLAN, shared multicast services will be provided to the multicast traffic within the range of SVGL multicast addresses. Other multicast traffic will be discarded.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

When the user VLAN is set to a shared VLAN or sub VLAN, shared multicast services are provided; when a user VLAN is set to other VLANs, independent multicast services are provided.

This mode is not supported in wireless environment and only the IVGL working mode is supported.

IVGL-SVGL

IVGL-SVGL mode is also called the hybrid mode. In this mode, a device running IGMP snooping can provide both shared and independent multicast services to the user VLAN.

- In a shared VLAN and sub VLAN, multicast services will be provided to the multicast traffic within an SVGL profile. For other multicast traffic, independent multicast services will be provided.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

When a user VLAN is configured as a shared VLAN or sub VLAN, both public multicast services and independent multicast services available. When a user VLAN is configured as a VLAN other than shared VLAN and sub VLAN, only the independent multicast services are available.

This mode is not supported in wireless environment and only the IVGL working mode is supported.

Related Configuration

Enabling IGMP Snooping and Selecting a Working Mode

IGMP snooping is disabled by default.

Run the **ip igmp snooping ivgl** command to enable IGMP snooping in IVGL mode.

Run the **ip igmp snooping svgl** command to enable IGMP snooping in SVGL mode.

Run the **ip igmp snooping ivgl-svgl** command to enable IGMP snooping in IVGL-SVGL mode.

A working mode must be designated when enabling IGMP snooping, namely, one of the preceding working modes must be selected.

Configuring Shared VLAN

The shared VLAN is VLAN 1 by default.

Run the **ip igmp snooping svgl vlan** command to designate a VLAN as the shared VLAN.

In SVGL mode and IVGL-SVGL mode, only one VLAN can be configured as the shared VLAN.

Configuring Sub VLAN

By default, a sub VLAN is any VLAN except the shared VLAN.

Run the **ip igmp snooping svgl subvlan** command to designate a VLAN as the sub VLAN.

In SVGL mode and IVGL-SVGL mode, the number of sub VLANs is not limited.

Configuring an SVGL Profile

No default setting.

Run the **ip igmp snooping svgl profile** *profile_num* command to configure the address range of an SVGL profile.

In SVGL mode and IVGL-SVGL mode, the SVGL profile range must be configured; otherwise, shared multicast services cannot be provided.

5.3.3 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier. In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1, IGMPv2, or IGMPv3.

Configuring the Source IP Address of a Querier

You can configure the source IP address of a query packet sent by the querier based on VLANs.

When the source IP address of the querier is not configured, the querier will not take effect.

Configuring the Query Interval of a Querier

You can configure the intervals for sending global Query packets based on different queriers on different VLANs.

Configuring the Maximum Response Time of a Query Packet

You can configure the maximum response time carried by a Query packet that is sent by a querier. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1. You can configure different maximum response time for queriers on different VLANs.

Configuring the Aging Time of a Querier

When other IGMP queriers exist on a network, the existing device will compete with other queriers. If the existing device fails to be elected and is in the non-querier state, the aging timer of a querier will be enabled. After the timer expires, other queriers on the network are considered as expired and the existing device will be resumed as the querier.

Related Configuration

Enabling the Querier Function

By default, the querier function of a device is disabled.

Run the **ip igmp snooping querier** command to enable the global querier function.

Run the **ip igmp snooping vlan** *num* **querier** command to enable the querier function for specific VLANs.

Specifying the IGMP Version for a Querier

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

Configuring the Source IP Address of a Querier

By default, the source IP address of a querier is 0.

Run the ip igmp snooping querier address command to enable global source IP addresses of queriers.

Run the ip igmp snooping vlan querier address command to specify the source IP addresses of the queriers on specific VLANs.

Configuring the Query Interval of a Querier

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan querier query-interval** to specify the global query interval of the queriers on specific VLANs.

Configuring the Maximum Response Time of a Query Packet

By default, the maximum response time of a query packet is 10s.

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to configure the aging time of queriers on specific VLANs.

5.3.4 Multicast-to-Unicast Conversion

The multicast-to-unicast conversion function is available only in wireless environment. After the function is configured on a wireless device, multicast packets between an AP and STAs are transmitted in unicast mode. The multicast-to-unicast conversion function runs on the AP.

Working Principle

The following describes the working principle of multicast-to-unicast conversion from several scenarios in wireless environment.

In fat AP mode, IGMP Snooping needs to learn and track user information. After multicast-to-unicast conversion is configured, the wireless multicast fast forwarding module queries the users who need multicast-to-unicast conversion through the interface provided by the multicast-to-unicast conversion module, and replaces the destination MAC addresses in multicast packets of the users with the MAC addresses of STAs, and destination IP addresses with IP addresses of the STAs, and then forwards the multicast packets in unicast mode.

In fit AP centralized forwarding mode, an AC, according to recorded user information, queries the WLAN ID and RADIO ID of an STA for packets, conducts CAPWAP encapsulation on the packets, and then sends the packets to an AP. If the multicast-to-unicast conversion is enabled, packets sent to the AP are delivered to the wireless multicast fast forwarding module, which queries the interface of the multicast-to-unicast conversion module to learn about the users who need multicast-to-unicast conversion. Then, the AP transmits multicast packets in unicast mode.

In fit AP local forwarding mode, after packets are forwarded to an AP, if multicast-to-unicast conversion is enabled, the AP delivers the packets to the wireless multicast fast forwarding module, which transmit multicasts the packets in unicast mode.

Related Configuration

↘ Enabling the Global Multicast Function

By default, the global multicast function is disabled. Run the **ip multicast wlan** command to enable the global multicast function. After global multicast is enabled, when an AC receives multicast packets, it conducts CAPWAP encapsulation on the multicast packets and sends the packets to the AP associated with the AC in CAPWAP unicast mode.

Run the **no ip multicast wlan** command to restore default configuration. After global multicast is disabled, an AC directly discards the received multicast packets.

↘ Enabling Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is disabled.

In ap-config mode on an AC, run the **igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion, or on a fat AP, run the **ip igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion.

In ap-config mode on an AC, run the **no igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion, or on a fat AP, run the **no ip igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion.

Configuring the Multicast Range for Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is available to all multicast profiles.

Use AC as an example. In ap-config mode, run the **igmp snooping mcast-to-unicast group-range** command to configure the profile address range for multicast-to-unicast conversion.

In ap-config mode, run the **no igmp snooping mcast-to-unicast group-range** command to restore the default configuration.

Configuring the Maximum Number of Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion can be configured for a maximum of 64 multicast profiles.

Use AC as an example. In ap-config mode, run the **igmp snooping mcast-to-unicast max-group** command to configure the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.

In ap-config mode, run the **no igmp snooping mcast-to-unicast max-group** command to restore the default configuration.

5.3.5 Optimizing the Multicast Wireless Environment

Ignoring port timer resetting for query packets refers to not resetting the port aging timer when a device receives query packets.

When multiple STAs are configured in a congested wireless network, after an AP sends out a query packet, the IGMP report packet responded by STAs may be discarded or the STAs fail to receive the query packet, and as a result, the AP fails to receive responses from the STAs. Traffic interruption may occur on the STAs. In this case, this function can be configured, in combination with aging time configuration of member ports, to ensure that an STA does not age within multiple query intervals. If an IGMP report packet from the STA is received within the query intervals, the port timer time is reset as the port aging time.

The configuration takes effect when query packets are received next time. A port timer that has been reset on a port will not be cancelled. The configuration prolongs aging time. Use it in appropriate scenarios.

The function is disabled by default.

Use AC as an example. In ap-config mode, run the **igmp snooping ignore-query-timer** command to ignore the port aging timer resetting for query packets.

In ap-config mode, run the **no igmp snooping ignore-query-timer** command to restore the default configuration.

5.4 Configuration

Configuration	Description and Command

Configuring Basic IGMP Snooping Functions (IVGL Mode)	Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode.	
	ip multicast wlan	Enables multicast globally.
	ip igmp snooping	Enables global IGMP snooping globally.
	igmp snooping	Enables multicast for an AP.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
Configuring the Packet Processing	(Optional) It is used to adjust relevant configurations for processing protocol packets.	
	ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-id*	Configures a static router port.
	p igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	Configures a static member port.
	ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**	Enables dynamic router port learning.
	ip igmp snooping dyn-mr-aging-time *time*	Configures the aging time of a dynamic router port.
	ip igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	ip igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
Configuring an IGMP Querier	(Optional) It is used to enable IGMP querier function on a network without a Layer-3 multicast device.	
	ip igmp snooping querier	Enables global querier function.
	ip igmp snooping vlan *num* **querier**	Enables the querier for a VLAN.
	ip igmp snooping querier version *num*	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan *num* **querier version** *num*	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address a.b.c.d	Configures the source IP address of queriers globally.
	ip igmp snooping vlan *num* **querier address** a.b.c.d	Configures the source IP address for a querier of a VLAN.

	ip igmp snooping querier query-interval *num*	Configures the query interval of queriers globally.
	ip igmp snooping vlan *num* **querier query-interval** *num*	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time *num*	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan *num* **querier max-response-time** *num*	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry *num*	Configures the aging timer for queriers globally.
	ip igmp snooping vlan *num* **querier timer expiry** *num*	Configures the aging timer for a querier of a VLAN.
Configuring Multicast-to-Unicast Conversion	**igmp snooping mcast-to-unicast enable**	Enables multicast-to-unicast conversion.
	igmp snooping mcast-to-unicast group-range *ip-addr ip-addr*	Configures the maximum multicast range for multicast-to-unicast conversion.
	igmp snooping mcast-to-unicast max-group *group-num*	Configures the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.
Optimizing the Wireless Multicast Environment	**ip igmp snooping ignore-query-timer**	Ignores the query timer.

5.4.1 Configuring Basic IGMP Snooping Functions (IVGL Mode)

Configuration Effect

- Enable IGMP snooping to realize Layer-2 multicast.
- Provide independent multicast services to each VLAN.

Notes

- IP multicast cannot be realized in SVGL mode. If IP multicast must be used, select the IVGL mode.
- PIM snooping must be run in IVGL mode. If PIM snooping must be run, select IVGL mode.

Configuration Steps

↘ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

If not specified, it is advised to run global IGMP snooping on all the devices connected user hosts.

Disabling IGMP Snooping for a VLAN

(Optional) You can use this function if you wish to disable IGMP snooping on specified VLANs.

Only when global IGMP snooping is enabled can it be disabled on specified VLANs.

In IVGL mode, each VLAN can enjoy independent multicast services. Disabling any VLAN multicast services will not interfere in the services provided to the others.

Verification

- Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table and verify that the member ports include only those connecting member hosts.
- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL mode.

Related Commands

Enabling Multicast Globally

Command	**ip multicast wlan**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, global multicast is disabled. This command must be configured before you configure the **IGMP snooping** command.

Enabling IGMP Snooping Globally

Command	**ip igmp snooping**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs. By default, IGMP snooping is disabled.

Enabling Multicast on the AP

Command	**igmp snooping**
Parameter	N/A

Description	
Command Mode	AP configuration mode
Usage Guide	By default, IGMP snooping is disabled.

Disabling IGMP Snooping for a VLAN

Command	**no ip igmp snooping vlan** *num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

Displaying the IGMP Snooping Entry

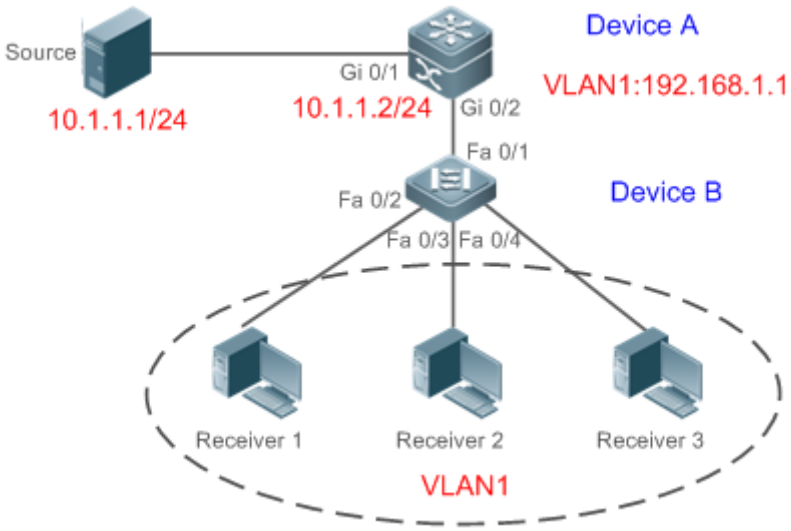
Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: `IGMP Snooping running mode: IVGL`

Configuration Example

Providing Layer-2 Multicast Services for the Subnet Hosts

Scenario **Figure 5-7**	
	A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)# ip igmp snooping ivgl
Verification	Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G. ● Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Fa0/2. ● Check whether the IGMP snooping working mode is IVGL.

B

```
B# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(D)
```

```
B# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

Common Errors

- The working mode of IGMP snooping is improper.

5.4.2 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.
- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network.
- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.
- Configure IGMP Snooping V3 to process all information in IGMPv3 packets.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

↘ Configuring a Static Router Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

↘ Configuring a Static Member Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

↘ Enabling Report Packet Suppression

- Optional.

- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

Enabling the Immediate-Leave Function

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

Disabling Dynamic Router Port Learning

- Optional.
- This function is used when multicast traffic needs to be forwarded only within the Layer-2 topology but not to a Layer-3 router.

Configuring the Aging Time of a Dynamic Router Port

- Optional.
- You can configure the aging time based on network load.

Configuring the Aging Time of a Dynamic Member Port

- Optional.
- You can configure the aging time based on the interval for sending IGMP query packets by the connected multicast router. Typically, the aging time is calculated as follows: Interval for sending IGMP query packets x 2 + Maximum response time of IGMP packets

Configuring the Maximum Response Time of a Query Packet

- Optional.
- You can configure the aging time based on network load.

Configuring IGMP Snooping v3

- Optional.
- Configure IGMP Snooping v3 to process all information in IGMPv1, IGMPv2, and IGMPv3 packets.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

Configuring a Static Router Port

Command	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	In SVGL mode, if a sub VLAN is not configured, only the configurations for the static router port within the shared VLAN can take effect, and the others can be configured but cannot take effect. If a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL-SVGL mode, if a sub VLAN is not configured, the configurations for the static router ports within all the VLANs can take effect; if a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.

Configuring a Static Member Port

Command	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *group-address*: Indicates a profile address. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

Enabling Report Packet Suppression

Command	**ip igmp snooping suppression enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

Enabling the Immediate-Leave Function

Command	**ip igmp snooping fast-leave enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address. The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.

Enabling Dynamic Router Port Learning

Command	**ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A router port is the port that is connected directly to a multicast device running IGMP snooping and a multicast neighbor device running multicast routing protocol. By default, dynamic router port learning is enabled and the device automatically listens to IGMP Query packets, DVMRP packets, and PIM Hello packets.

Configuring the Aging Time of a Dynamic Member Port

Command	**ip igmp snooping host-aging-time** *seconds*
Parameter Description	*seconds*: Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile. When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.

Configuring the Maximum Response Time of a Query Packet

Command	**ip igmp snooping query-max-response-time** *seconds*
Parameter Description	*seconds*: Indicates the maximum response time.
Command Mode	Global configuration mode

Displaying Router Ports

Command	**show ip igmp snooping mroute**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the router port is successfully configured, an "S" will be displayed in the port information. `Ruijie(config)#show ip igmp snooping mrouter` `Multicast Switching Mroute Port` `  D: DYNAMIC` `  S: STATIC` `(*, *, 1):` `  VLAN(1)  1 MROUTES:` `    GigabitEthernet 0/1(S)`

Displaying the Information of Dynamic Router Port Learning

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time and learning status of the dynamic router port. `Dynamic Mroute Aging Time : 300(Seconds)` `Multicast router learning mode: pim-dvmrp`

Displaying the Information of a Member Port

Command	**show ip igmp snooping gda-table**

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the member port is successfully configured, an "S" will be displayed in the port information. `Ruijie(config)#show ip igmp snooping gda-table` `Multicast Switching Cache Table` `D: DYNAMIC` `S: STATIC` `M: MROUTE` `(*, 224.1.1.1, 1):` `VLAN(1) 1 OPORTS:` `GigabitEthernet 0/1(S`

Displaying Other Parameters

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave. `IGMP Fast-Leave: Enable` `IGMP Report suppress: Enable` `Query Max Response Time: 20(Seconds)` `Dynamic Mroute Aging Time : 300(Seconds)` `Dynamic Host Aging Time : 260(Seconds)`

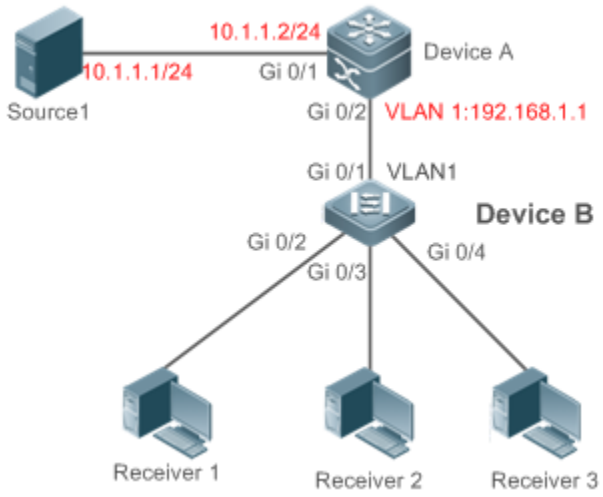
Configuration Example

Configuring a Static Router Port and Static Member Port

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.

	Ruijie# configure terminal Ruijie(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Ruijie(config)# end
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.
	Ruijie#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S) Ruijie#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM)

Enabling Report Packet Suppression

Scenario **Figure 5-8**	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Enable Report packets suppression on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable
Verification	Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.

B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Configuring Other Parameters

Configuration Steps	• Configure basic IGMP snooping functions. • Enable Immediate-leave function. • Disable router port learning. • Configure the aging time of a router port. • Configuring the aging time of a member port. • Configure the response time of a Query packet.
	Ruijie# configure terminal Ruijie(config)# ip igmp snooping fast-leave enable Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp Ruijie(config)#ip igmp snooping dyn-mr-aging-time 200 Ruijie(config)#ip igmp snooping host-aging-time 100 Ruijie(config)#ip igmp snooping query-max-response-time 60 Ruijie(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.
	Ruijie#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536

	Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 200(Seconds) Dynamic Host Aging Time : 100(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

5.4.3 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

↘ Enabling the Querier Function

- (Optional) Enable IGMP querier function globally or for a specified VLAN.
- (Optional) Disable the IGMP querier function for a specified VLAN.

↘ Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.

↘ Configuring the Maximum Response Time of a Query Packet

- (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.

Configuring the Query Interval of a Querier

- (Optional) Adjust the interval of the IGMP querier for sending query packets.

Configuring the Aging Timer of a Querier

- (Optional) Configure the aging timer of other IGMP queriers on the network.

Specifying the IGMP Version for a Querier

- (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

Enabling the IGMP Querier Function

Command	**ip igmp snooping** [**vlan** *vid*] **querier**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

Configuring the Source IP Address of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *a.b.c.d*: Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

Configuring the Maximum Response Time of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*

Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Query Interval of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Aging Timer of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

Specifying the IGMP Version for a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier version 1**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

Displaying the IGMP Querier Configuration

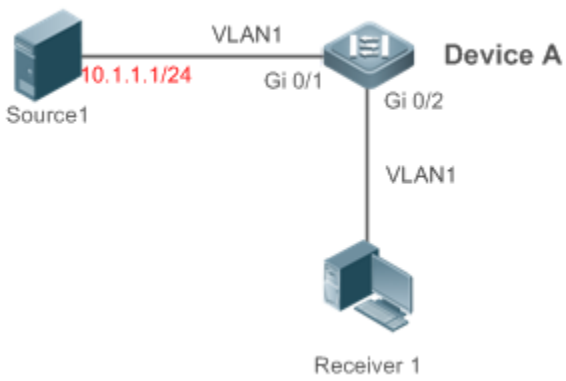
Command	**show ip igmp snooping querier detail**

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed.

```
Ruijie(config)#show ip igmp snooping querier detail

Vlan      IP Address           IGMP Version           Port

-----------------------------------------------------------


Global IGMP switch querier status

-----------------------------------------------------------

admin state                    : Enable

admin version                  : 2

source IP address              : 1.1.1.1

query-interval (sec)           : 60

max-response-time (sec)        : 10

querier-timeout (sec)          : 125


Vlan 1:   IGMP switch querier status

-----------------------------------------------------------

admin state                    : Disable

admin version                  : 2

source IP address              : 1.1.1.1

query-interval (sec)           : 60

max-response-time (sec)        : 10

querier-timeout (sec)          : 125

operational state              : Disable

operational version            : 2
```

Configuration Example

↘ Enabling the IGMP Querier Function

Scenario **Figure 5-9**	
	In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.
Configuration Steps	● Enable global IGMP snooping on A in IVGL mode. ● Enable IGMP querier for VLAN 1 on A.
A	`A(config)#ip igmp snooping ivgl` `A(config)#ip igmp snooping querier` `A(config)#ip igmp snooping querier address 10.1.1.1` `A(config)#ip igmp snooping vlan 1 querier`
Verification	Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.
A	`A(config)#show ip igmp snooping querier` `Vlan IP Address IGMP Version Port` `---` `1 10.1.1.1 2 switch` `A(config)#show ip igmp snooping querier vlan 1` `Vlan 1: IGMP switch querier status` `---` `elected querier is 10.1.1.1 (this switch querier)` `---` `admin state : Enable`

```
admin version                : 2
source IP address            : 10.1.1.1
query-interval (sec)         : 60
max-response-time (sec)      : 10
querier-timeout (sec)        : 125
operational state            : Querier
operational version          : 2
```

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

5.4.4 Configuring Multicast-to-Unicast Conversion

Configuration Effect

- Enable the multicast-to-unicast conversion on the AP, which transmits multicast packets to STAs in unicast mode.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

Enabling Global Multicast

- (Mandatory) Enable global multicast in global mode.
- If global multicast is disabled in global mode, a wireless device directly discards received packets.

Enabling Multicast-to-Unicast Conversion

- (Optional) Configure whether to enable multicast-to-unicast conversion. After multicast-to-unicast conversion is enabled, after packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode and transmits such packets in unicast mode.

Configuring the Multicast Range for Multicast-to-Unicast Conversion

- (Optional) Multicast-to-unicast conversion is available to all multicast groups by default. A multicast range can be configured to allow multicast packets to be transmitted in unicast mode, so as to utilize AP resources to the maximum extent.

Configuring the Maximum Number of Multicast Profiles that Are Allowed to Use Multicast-to-Unicast Conversion

- (Optional) The maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion can be adjusted.

- It is used in combination with the multicast range of multicast-to-unicast conversion.

Verification

- Run the show ip igmp snooping command to check whether the configuration takes effect.

Related Commands

Configuring Global Multicast

Command	**ip multicast wlan**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If global multicast is enabled, multicast packets are processed only after they reach the AC. If global multicast is disabled, the AC directly discards the received multicast packets.

Configuring Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast enable**
Parameter Description	N/A
Command Mode	ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	After multicast-to-unicast conversion is enabled, when multicast packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode according to the multicast-to-unicast conversion policy.

Configuring the Maximum Multicast Range for Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast group-range** *ip-addr ip-addr*
Parameter Description	*ip-addr:* Indicates the multicast profile range. The value must be valid multicast addresses and ranges from 224.0.1.0 to 239.255.255.255.
Command Mode	Ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	If the multicast range of multicast-to-unicast conversion is not configured, multicast-to-unicast conversion is available to all multicast profiles by default.

Configuring the Maximum Number of Multicast Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast max-group** *number*

Parameter Description	number: Indicates the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion. The value ranges from 1 to 64. The default value is 64.
Command Mode	ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	It can be used in combination with the maximum multicast range of multicast-to-unicast conversion so as to properly allocate bandwidth and effectively control AP resources.

Displaying Multicast-to-Unicast Conversion Configuration

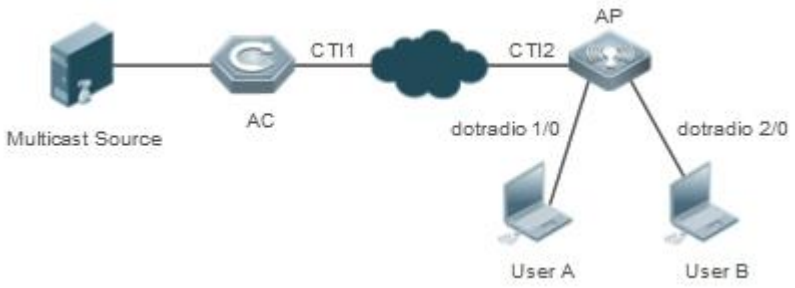
Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	If multicast-to-unicast conversion is configured successfully, the following information is displayed:

```
Ruijie(config)#sh ip igmp snooping

WLAN Multicast: Enable

IGMP Snooping running mode: IVGL

IGMP Snooping M2U-Forward: Enable

IGMP Snooping Support M2U Max-Group Num: 64

IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64

IGMP Snooping L2-entry-limit: 65536

Source port check: Disable

Source ip check: Disable

IGMP Fast-Leave: Disable

IGMP Report suppress: Disable

IGMP Global Querier: Disable

IGMP Preview: Disable

IGMP Tunnel: Disable

IGMP Preview group aging time : 60(Seconds)

Dynamic Mroute Aging Time : 300(Seconds)

Dynamic Host Aging Time : 260(Seconds)
```

Configuration Example

The following configuration example describes only configurations related to IGMP Snooping.

Enabling the IGMP Querier

Scenario **Figure 5-10**	
	Multicast streams only need to be forwarded at Layer 2 in network deployment and there is no device supporting the Layer-3 multicast function in the network. User A and User B are multicast receivers.
Configuration Steps	● Enable IGMP Snooping on the AC. ● Enable global multicast on the AC. ● Enable IGMP Snooping in ap-config mode. ● Enable multicast-to-unicast conversion in ap-config mode. ● Configure the maximum multicast range for multicast-to-unicast conversion in ap-config mode. ● Configure the maximum number of multicast profiles that are allowed to support multicast-to-unicast conversion in ap-config mode.
A	`A(config)#ip igmp snooping ivgl` `A(config)#ip multicast wlan` `A(config)#ap-confing all` `A(config-ap)#igmp snooping` `A(config)#igmp snooping mcast-to-unicast enable` `A(config-ap)#igmp snooping mcast-to-unicast group-range 233.1.1.1 233.255.255.255` `A(config-ap)#igmp snooping mcast-to-unicast max-group 10`
Verification	Run the **show ip igmp snooping** command to check whether the configuration takes effect.
A	`A(config)# sh ip igmp snooping` `WLAN Multicast: Enable` `IGMP Snooping running mode: IVGL` `IGMP Snooping M2U-Forward: Enable` `IGMP Snooping Support M2U Max-Group Num: 64` `IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64` `IGMP Snooping L2-entry-limit: 65536` `Source port check: Disable`

	Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Common Errors

- Multicast packets are not processed because global multicast is not configured.

5.4.5 Optimizing the Wireless Multicast Environment

Configuration Effect

- Configure the function of ignoring port timer resetting for query packets on the wireless device.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

↘ Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets

- (Optional) Configure the function of ignoring port aging timer resetting for query packets so that the port does not age within multiple query intervals.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

↘ Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets

Command	**ip igmp snooping ignore-query-timer**
Parameter Description	N/A
Command Mode	Global configuration mode or ap-config mode

Usage Guide	After the function of ignoring port aging timer for query packets is configured, the port does not age within multiple query intervals. When the port receives a Report request, the port aging timer resets.

5.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the dynamic router ports and member ports.	**clear ip igmp snooping gda-table**

Displaying

Description	Command
Displays basic IGMP snooping configurations.	**show ip igmp snooping** [**vlan** *vlan-id*]
Displays the router ports.	**show ip igmp snooping mrouter**
Displays the IGMP snooping entries.	**show ip igmp snooping gda-table**
Displays the IGMP querier.	**show ip igmp snooping querier** [**detail**]
Displays user information.	**show ip igmp snooping user-info**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all IGMP Snooping functions.	**debug igmp-snp**
Debugs the IGMP snooping events.	**debug igmp-snp event**
Debugs the IGMP snooping packets.	**debug igmp-snp packet**
Debugs the communications between IGMP snooping and MSF.	**debug igmp-snp msf**
Debugs the IGMP snooping alarms.	**debug igmp-snp warning**

Security Configuration

1. Configuring Web Authentication
2. Configuring AAA
3. Configuring RADIUS
4. Configuring 802.1X
5. Configuring ARP Check
6. Configuring Gateway-targeted ARP Spoofing Prevention
7. Configuring Global IP-MAC Binding
8. Configuring DHCP Snooping
9. Configuring IP Source Guard
10. Configuring DNS Snooping
11. Configuring Port Security
12. Configuring VRRP
13. Configuring IGMP Snooping
14. Configuring the ACL

15. Configuring TACACS+
16. Configuring SCC
17. Configuring Password Policy
18. Confugring SSH
19. Configuring GSN
20. Configuring SUMNG

1 Configuring Web Authentication

1.1. Overview

1.1.1. Web Authentication

Web authentication controls user access to networks. It requires no authentication software on clients. Instead, users can perform authentication on common browsers.

When unauthenticated clients attempt to access the Internet using browsers, the network access server (NAS) forcibly redirects the browsers to a specified site pointing to a Web authentication server, also called a portal server. Users can access the services on the portal server before being authenticated, such as downloading security patches and reading notices. If a user wants to access network resources beyond the portal server, the user must get authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server performs Webpage interaction with browsers, providing personalized services, such as advertisements, notices, and business links on the authentication page.

Ruijie Web Authentication Versions

There are three versions of Ruijie Web authentication, including Ruijie First-Generation Web Authentication, Ruijie Second-Generation Web Authentication, and Ruijie Internal Portal (iPortal) Web Authentication. The Web authentication process varies with authentication versions. For details, see Section 1.3 "Features".

⚠ The three versions of Web authentication are highly divergent in features and configurations. It is recommended to read through the relevant chapters carefully before configuration.

⚠ Both Ruijie Second-Generation Web Authentication and Ruijie iPortal Web Authentication support local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is more commonly used in reality, it is used as an example in the chapter "Applications".

⚠ The concept of "interface" varies with product types. For example, the interfaces on a layer-2 switch are physical ports; the interfaces on a router may be sub interfaces; the interfaces on wireless devices may represent a wireless local area network (WLAN). This document uses the unified term "interface" to include them. In application, recognize the real meaning based on specific products and functions.

⚠ Web authentication supports user online traffic detection. For details, see the Configuring SCC.

⚠ Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see the Configuring AAA.

Protocols and Standards

- HTTP: RFC1945 and RFC2068

- HTTPS: RFC2818
- SNMP: RFC1157 and RFC 2578
- RADIUS: RFC2865, RFC2866, and RFC3576
- For the standards related to MAC SMS authentication, see the *CMCC WLAN Device Interface Standards V3.1.0_20130901 (MAC Address-Based Authentication Extension), Zhejiang CMCCWLAN Fast Authentication Scheme – Interface Standards V1.1-2011.3.22*, and *WLAN Fast MAC Address-Based SMS Authentication Scheme V1.1-2011.3.21*.

1.2. Applications

Application	Description
Basic Scenario of Web Authentication	Basic layer-2 authentication scenario, where a NAS, portal server, and RADIUS server constitute an authentication system which connects a client with the NAS through the layer-2 network.

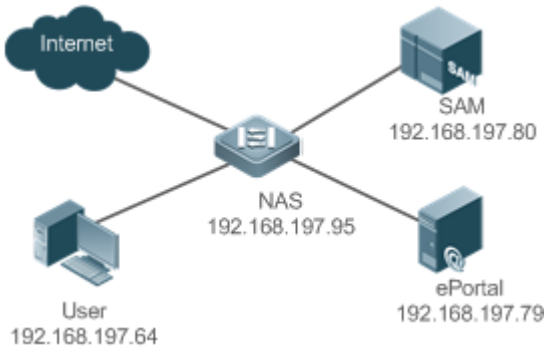
1.2.1. Basic Scenario of Web Authentication

Scenario

See Figure 1-1.

- Deploy a Web authentication scheme on the NAS.
- The client connected to the NAS needs to pass Web authentication before accessing the Internet.

Figure 1-1 Networking Topology of Web Authentication



Remarks	Web authentication is applicable to both layer-2 and layer-3 networks. At layer 3, the source MAC address and VID of a packet are changed after it is routed, but the source IP address remains the same as the only identifier of a client. Therefore, the binding policy of Web authentication on layer-3 devices must adopt the IP-only binding mode. Here, layer-2 NAS is used as an example. RG-SAM program is installed on the RADIUS server. RG-ePortal program is installed on the portal server.

Deployment

- Enable Web authentication on the client-accessed interface or globally on the NAS (globally on EG devices).
- Configure the ePortal server and the communication key on the NAS (for only Ruijie First-Generation and Second-Generation Web Authentication).
- Configure the Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only Ruijie First-Generation and Second-Generation Web Authentication).
- Configure the consistent communication parameters on the ePortal server and SAM server (for only Ruijie First-Generation Web Authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).
- Configure the IP address of the SAM server on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).
- Configure the names of the Web authentication method lists on the NAS (for only Ruijie Second-Generation and iPortal Web Authentication).

1.3. Features

Basic Concepts

Ruijie First-Generation Web Authentication

Ruijie First-Generation Web Authentication should cooperate with the RG-ePortal software. The server installed with RG-ePortal provides a login page to submit user authentication information, and initiates an authentication request to the RADIUS server directly. After authentication succeeds, the NAS gets user information delivered through the SNMP protocol, and thereby controls user access permissions. Communication during Web authentication of this version depends on private SNMP nodes. Moreover, the ePortal server takes the place of the NAS in authentication and accounting, which relieves the NAS from service burden.

Ruijie Second-Generation Web Authentication

Ruijie Second-Generation Web Authentication complies with the *CMCC WLAN Service Portal Specification*. The portal server is responsible only for Webpage interaction with users. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and the NAS complies with the *CMCC WLAN Service Portal Specification*. The portal server provides a login page for users to submit their information, and informs the NAS of user information through the portal protocols. The NAS completes authentication by interacting with the RADIUS server based on the user information, assigns access permissions to authenticated clients, and returns authentication results to the portal server.

The implementation process of Ruijie Second-Generation Web Authentication is mainly completed on the NAS. This raises a higher demand on the NAS's capability to handle heavy tasks. Meanwhile, the portal server is simplified. The standard *CMCC WLAN Service Portal Specification*, which gains highly industry support, enables various vendors to develop compatible products.

Ruijie iPortal Web Authentication

In Ruijie iPortal Web Authentication, the NAS integrates Webpage interaction of the portal server and partial authentication interaction of the RADIUS server. The NAS has a default authentication page suite. It can be customized according to the configuration described in this manual. Then, download the configured page suite to the storage medium of the NAS for effect.

Version Comparison

Authentication roles:

- Client: Its functions are the same among the three types of Web authentication.
- NAS: In Ruijie First-Generation Web Authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In Ruijie Second-Generation Web Authentication, the NAS is responsible for redirecting and authenticating users as well as notifying the portal server of authentication results. In Ruijie iPortal Web authentication, the NAS integrates multiple functions including the URL redirection, Webpage interaction, and authentication.
- Portal server: In Ruijie First-Generation Web Authentication, the portal server is responsible for interaction with clients through Webpages, authenticating users, and notifying the NAS of authentication results. In Ruijie Second-Generation Web Authentication, the portal server is responsible for interacting with clients through Webpages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS. In Ruijie iPortal Web Authentication, the portal server is built into the NAS and provides simplified functions, mainly responsible for Web page interaction with clients.
- RADIUS server: Its functions are the same among the three types of Web authentication.

Authentication process:

- In Ruijie Second-Generation Web Authentication, the authentication and accounting functions are transferred from the portal server to the NAS.
- Because authentication proceeds on the NAS, the second-generation NAS does not need to wait for the authentication results notified by the portal server as the first generation.
- Ruijie iPortal Web Authentication simplifies and integrates the features of the first- and second- generation portal servers into the NAS.

Logout process:

- In Ruijie First-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, or traffic detection or port status detection performed by the NAS. In Ruijie Second-Generation Web Authentication, a logout action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS. In Ruijie iPortal Web Authentication, a logout action may be triggered by the voluntary logout of a user through clicking the **Logout** button on the online page, a kickout notification from the RADIUS server, or traffic detection or port status detection performed by the NAS.
- In Ruijie First-Generation Web Authentication, Accounting Stop packets are sent by the portal server. In Ruijie Second-Generation Web Authentication, Accounting Stop packets are sent by the NAS, the same as Ruijie iPortal Web Authentication.

The selection of the Web authentication versions depends on the type of the portal server in use.

Command parameters in this document may be shared by the three Web authentication versions or not. Read through this document carefully to avoid parameter misconfiguration that will affect Web authentication.

Overview

Feature	Description
Ruijie First-Generation Web Authentication	The portal server is deployed and supports only Ruijie First-Generation Web Authentication.
Ruijie Second-Generation Web Authentication	The portal server is deployed and complies with the *CMCC WLAN Service Portal Specification*.
Ruijie iPortal Web Authentication	The portal server is not deployed, and the NAS supports Webpage interaction.

1.3.1. Ruijie First-Generation Web Authentication

HTTP Interception

HTTP interception means the NAS intercepts to-be-forwarded HTTP packets. Such HTTP packets are initiated by the browsers of the clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit the website www.google.com using the Internet Explorer, the NAS is expected to forward the HTTP request packets to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

After HTTP interception is successful, the NAS redirects the HTTP requests from the client to itself to establish a session between them. Then, the NAS pushes a Webpage to the client through HTTP redirection, which can be used for authentication, software downloading or other purposes.

You can specify the clients and destination interfaces to enable or disable HTTP interception for Web authentication. In general, HTTP requests from unauthenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the foundation of Web authentication. Web authentication is automatically triggered once HTTP interception succeeds.

HTTP Redirection

According to HTTP protocols, after the NAS receives a HTTP GET or HEAD request packet from a client, a packet with 200 (Ok) status code is replied if it is able to provide the required resources, or a packet with 302 (Moved Temporarily) status code is returned if unable. Another URL is provided in the 302 packet. After receiving the packet, the client may resend a HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is an important procedure following HTTP interception in Web authentication. It takes the advantage of 302 status code defined in HTTP protocols. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (which should have been sent to another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. Thereby, the client resends the requests to the redirection page.

Because more and more application programs run HTTP protocols, the use of the 302 redirection packet may divert a large amount of HTTP traffic (not sent by browsers) to the portal server, which will affect network authentication. To address this problem, HTTP redirection technology on the NAS adopts noise reduction to replace the 302 packets with the **js** script.

Working Principle

Figure 1-1 shows the networking topology of Web authentication.

First-generation Webauth roles:

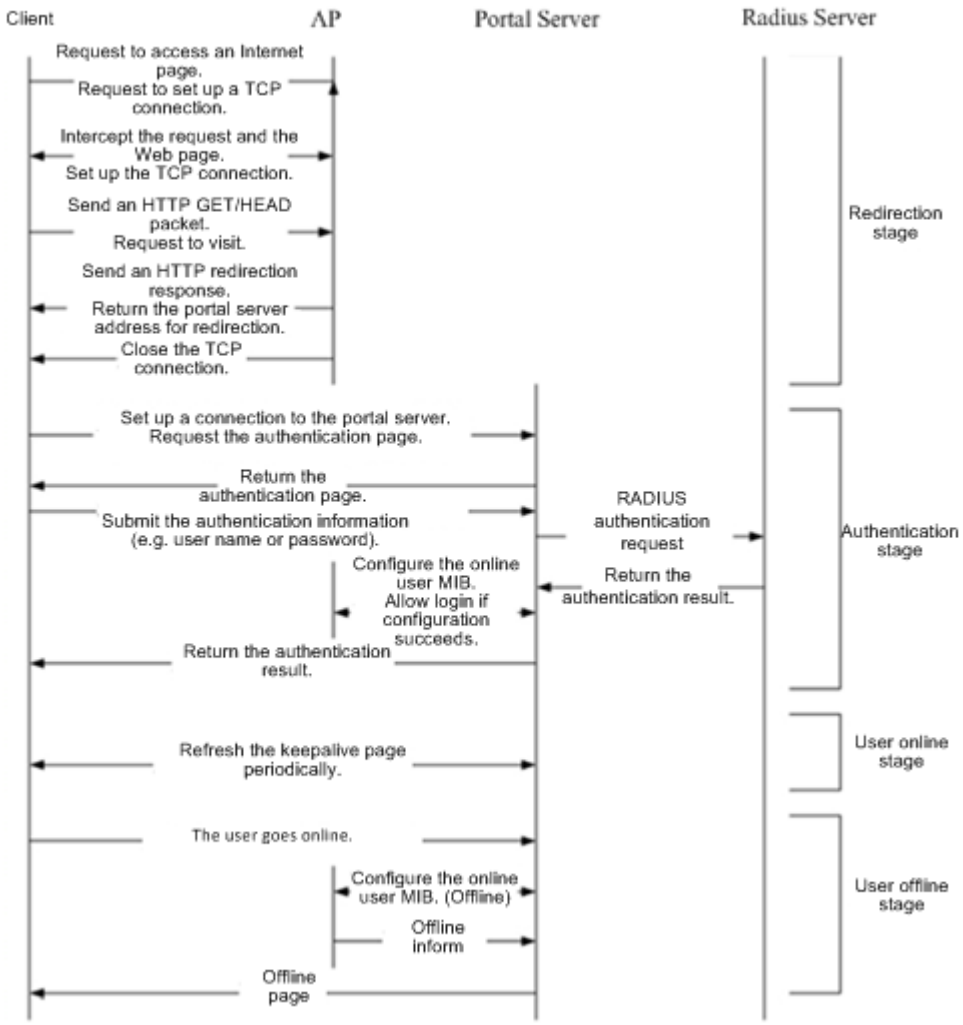
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network (for example, a wireless access point [AP] on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, sends the information to the RADIUS server for authentication, and notifies the client and NAS of the authentication result. Figure 1-1 shows Ruijie ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. The portal server extracts users' authentication account information from HTTP packets and initiates authentication requests to the RADIUS server through the RADIUS protocol. The RADIUS server returns the authentication result to the portal server through the RADIUS protocol. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

First-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server and complete authentication.
3. After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 1-2 shows the flowchart of Ruijie First-Generation Web Authentication by using an AP as the NAS.

Figure 1-2 Flowchart of Ruijie First-Generation Web Authentication



First-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. Scenario 1: The NAS detects a client to logout and informs the portal server. Then the portal server deletes the user information on the NAS through SNMP and displays a logout page to the client.
2. Scenario 2: The portal server detects a client to logout and informs the NAS through SNMP and displays a logout page to the client.
3. In the two scenarios, the portal server sends an Accounting Stop request to the RADIUS server and notifies the RADIUS server that the client has logged out.

Related Configuration

↘ Configuring the First-Generation Webauth Template

By default, the first-generation Webauth template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** {*string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling Ruijie First-Generation Web Authentication

By default, Ruijie First-Generation Web Authentication is disabled.

Run the **web-auth enable** command in interface configuration mode to enable Ruijie First-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Configuring the SNMP-Server Host

By default, the SNMP-server host and community string are not configured.

Run the **snmp-server host** {*ip-address* }**version 2c** {*community-string* }**web-auth** command in global configuration mode to configure the SNMP-server host and community string for Web authentication.

The SNMP-server host is configured to receive Inform/Trap packets of user logout.

Configuring the SNMP-Server Community String

By default, the SNMP-server community string is not configured.

Run the **snmp-server community** {*community-string*} **rw** command in global configuration mode to configure the SNMP-server community string.

The SNMP-server community string is configured to read/write user information from/to the NAS.

Enabling the SNMP Trap/Inform Function

By default, the SNMP Trap/Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap/Inform function.

The SNMP Trap/Inform function is configured to enable the NAS to inform the portal server of user logout.

1.3.2. Ruijie Second-Generation Web Authentication

HTTP Interception

Same as the HTTP interception technology of Ruijie First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of Ruijie First-Generation Web Authentication.

Working Principle

Figure 1-1 shows the networking topology of Web authentication.

Second-generation Webauth roles:

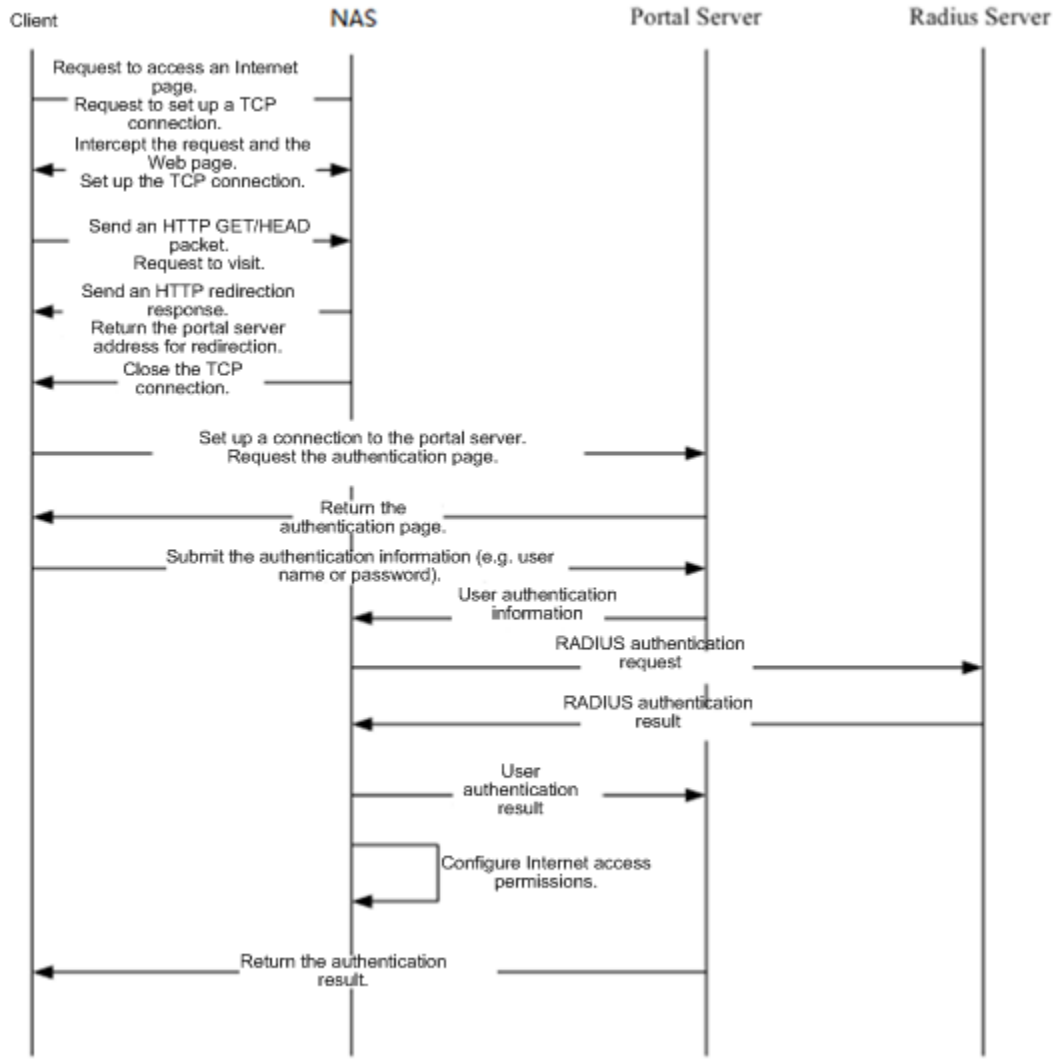
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication. The NAS receives user authentication information from the portal server, sends authentication requests to the RADIUS server, determines whether users can access the Internet according to authentication results, and returns the authentication results to the portal server.
3. Portal server: Provides a Web page for Web authentication and related operations. After receiving an HTTP authentication request from a client, the portal server extracts account information from the request, transfers the information to the NAS, and displays the authentication result returned by the NAS to the user on a page. Figure 1-1 shows Ruijie ePortal server.
4. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

Second-generation Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.

2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.
3. The portal server sends the user authentication information to the NAS.
4. The NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.
5. The portal server displays the authentication result (success or failure) to the user on a page.

Figure 1-3 Flowchart of Ruijie Second-Generation Web Authentication



Second-generation client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page or the keep-alive page is invalid.

1. When a user clicks the **Logout** button on the online page, the portal server notifies the NAS to get the user offline.

2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
3. When the RADIUS server plans to force a client offline based on a certain policy, the NAS notifies the portal server to push a logout page to the client.

Related Configuration

Configuring the Second-Generation Webauth Template

By default, the second-generation Webauth template is not configured.

Run the **web-auth template{eportalv2 |** *template-name* **v2}** command in global configuration mode to create a second-generation Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** {*url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Configuring the Webauth Communication Key

By default, the Webauth communication key is not configured.

Run the **web-auth portal key** { *string* } command in global configuration mode to configure the Webauth communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling Ruijie Second-Generation Web Authentication

By default, Ruijie Second-Generation Web Authentication is disabled.

Run the **web-auth enable {eportalv2 |** *template-name* **v2}** command in interface configuration mode to enable Ruijie Second-Generation Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie Second-Generation Web Authentication relies on AAA. Enable AAA before you implement the former.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host is responsible for authenticating users.

Configuring an AAA Method List for Ruijie Second-Generation Web Authentication

By default, no AAA method list is configured for Ruijie Second-Generation Web Authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for Ruijie Second-Generation Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

Configuring an AAA Method List for Ruijie Second-Generation Web Accounting

By default, no AAA method list is configured for Ruijie Second-Generation Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie Second-Generation Web Accounting.

The AAA method list for Web accounting is used for accounting interaction during the Webauth process.

Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

Specifying the UDP Port of the Portal Server

By default, UDP Port 50100 is used.

Run the **port** command in template configuration mode to specify the UDP port of the portal server.

The UDP port is specified for the portal server to communicate with the NAS.

1.3.3. Ruijie iPortal Web Authentication

HTTP Interception

Same as the HTTP interception technology of Ruijie First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of Ruijie First-Generation Web Authentication.

Working Principle

Compared with Ruijie First-Generation Web Authentication shown in Figure 1-1, Ruijie iPortal Web Authentication does not require the portal server.

iPortal Webauth roles:

1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network. It is directly connected to clients in wired or wireless networks and must be enabled with Ruijie iPortal Web Authentication. The NAS resolves the account information that clients enter on a Webpage and sends authentication requests to the RADIUS server. It determines whether clients can access the Internet according to authentication results and pushes the authentication results to the browsers.
3. RADIUS server: Provides the RADIUS-based authentication service to remote clients. Figure 1-1 shows the RADIUS server installed with the RG-SAM program.

iPortal Webauth process:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the iPortal server (NAS).
3. The NAS initiates authentication to the RADIUS server and displays the authentication result (success or failure) to the client on a page.

Client logout process:

1. The NAS gets a client offline after the **Logout** button on the Web page is clicked.
2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
3. When the RADIUS server forces a client offline based on a certain policy, the NAS pushes a logout page to the client.

Related Configuration

↘ **Configuring the iPortal Webauth Template**

By default, the iPortal Webauth template is not configured.

Run the **web-auth template iportal** command in global configuration mode to create an iPortal Webauth template.

The template is used to configure authentication-related parameters on the iPortal server.

Customizing a Page Suite

By default, the factory file package is used.

Run the **page-suite** command in template configuration mode to specify the use of a page suite.

Before you specify the use of a page suite, download it to the flash memory.

Configuring an Advertisement URL and Mode

By default, advertisement pops up after login.

In template configuration mode, run the **login-popup** *url* command to configure the advertisement URL and specify pre-login mode; run the **online-popup** *url* command to configure the advertisement URL and specify post-login mode.

Specifying the Webauth Binding Mode

The default Webauth binding mode is IP-MAC binding mode.

Run the **bindmode** command in template configuration mode to specify the Webauth binding mode.

In Web authentication on layer-3 networks, the source MAC address in a packet is changed after the packet is routed. In such case, configure the IP-only binding mode.

Enabling Ruijie iPortal Web Authentication

By default, Ruijie iPortal Web Authentication is disabled.

Run the **web-auth enable iportal** command in interface configuration mode to enable Ruijie iPortal Web Authentication on the client-connected ports.

After Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie iPortal Web Authentication relies on AAA. Enable AAA before you implement Web authentication.

Configuring the RADIUS-Server Host and Communication Key

By default, the RADIUS-server host and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS-server host and communication key.

The RADIUS-server host in Web authentication is responsible for authenticating users.

Configuring an AAA Method List for Ruijie iPortal Web Authentication

By default, no AAA method list is configured for Ruijie iPortal Web Authentication.

Run the **aaa authentication iportal** command in global configuration mode to configure an AAA method list for Ruijie iPortal Web Authentication.

The AAA authentication method list is used for interaction during the Webauth process.

↘ Configuring an AAA Method List for Ruijie iPortal Web Accounting

By default, no AAA method list is configured for Ruijie iPortal Web Accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie iPortal Web Accounting.

The AAA accounting method list is used for accounting interaction during the Webauth process.

↘ Specifying an AAA Method List

The default AAA method list is used if no list is specified.

Run the **authentication** command in template configuration mode to specify an AAA method list.

The AAA method list is specified to send authentication requests to AAA.

↘ Specifying an AAA Accounting Method List

The default AAA accounting method list is used if no list is specified.

Run the **accounting** command in template configuration mode to specify an AAA accounting method list.

The AAA accounting method list is specified to send accounting requests to AAA.

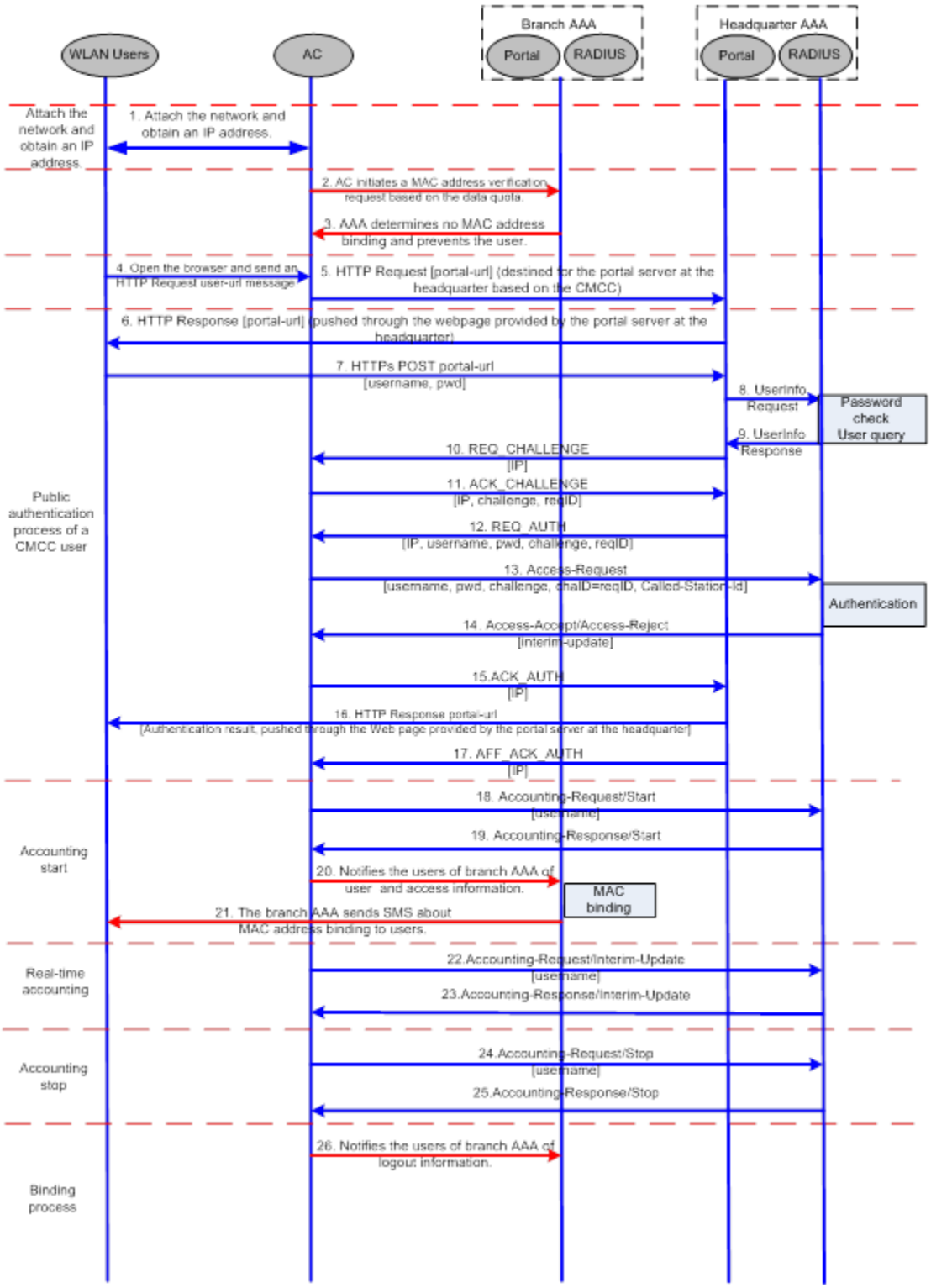
1.3.4. Ruijie MAC Address-Based SMS Authentication

Working Principle

After an STA is associated with an SSID enabled with MAC address-based SMS authentication, the STA obtains an IP address through the Dynamic Host Configuration Protocol (DHCP). Then the STA is allowed to access the Internet. When the STA uses up the traffic allowed during a time period, the access controller (AC) initiates a MAC address binding query to the bound portal server. If the STA is bound with a MAC address, the portal server sends an authentication request. If the STA is not bound with a MAC address, the STA needs to re-perform authentication on the portal server before accessing the Internet.

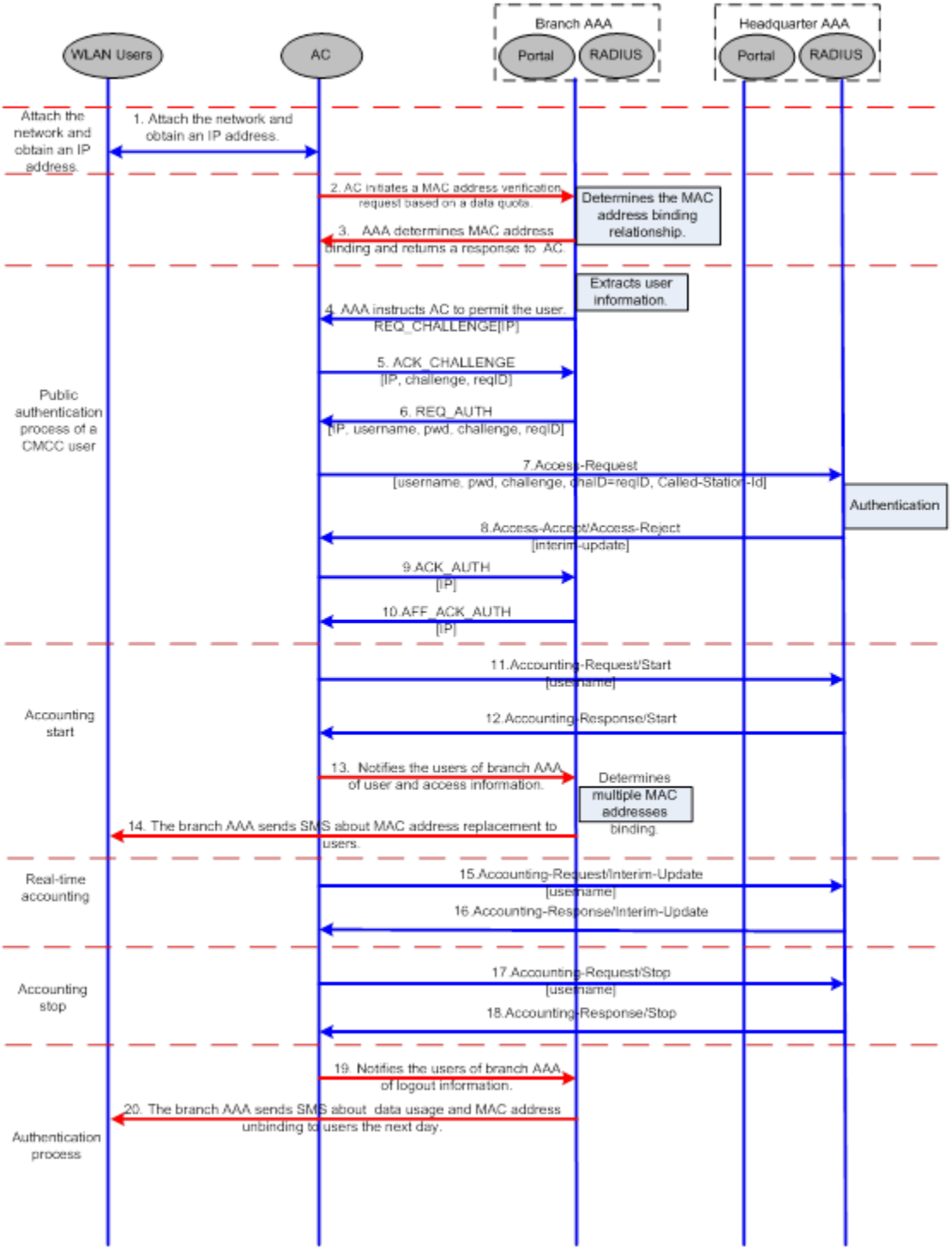
↘ SMS Authentication Process for Unbound STAs

The following figure shows the process where an STA not bound with a MAC address associates the SSID enabled with MAC address-based SMS authentication to access the Internet. Compared with Ruijie Second-Generation Web Authentication, MAC address-based SMS authentication is added with the procedures of querying MAC address binding and notifying the bound portal server of user login/logout. The rest of the process is the same. If the STA selects the **Bind** check box when performing authentication on the portal server, the portal server will bind the STA with a MAC address. Next time the STA can access the Internet directly.



SMS Authentication Process for Bound STAs

After an STA is bound with a MAC address, the user does not need to open the browser to perform authentication for Internet access. Network access is automatically completed after the STA is associated with a network, which greatly facilitates wireless network access.



1.3.5. RIPT Web Authentication

Web authentication on wireless devices supports the Remote Intelligent Perception Technology (RIPT) function. When an AC is faulty or the AC is disconnected from an AP, the Web authentication function on the AP continues to provide the authentication service externally.

Working Principle

To enable RIPT, configure an RIPT AP group on an AC. For details, see the *Configuring RIPT*. In RIPT AP authentication mode, the configurations related to Web authentication on the AC are issued to the APs. The AP can function as access devices to provide the Web authentication service externally. (STAs do not need to perform Web authentication on the AC.) The information of the clients who pass authentication on the APs is synchronized to the AC and can be viewed on the AC.

↘ Issuing Configurations

In RIPT AP authentication mode, the configurations of AAA and RADIUS on the AC and port-based Web authentication control in RSNA will be issued to the APs. After that, the APs can provide WLAN services externally, including the Web authentication service.

↘ Synchronizing Client Information from the APs to the AC

If clients pass authentication by an RIPT AP which provides the Web authentication service externally, the information of the clients will be synchronized to the AC and can be viewed on the AC.

1.3.6. WiFiDog Web Authentication

HTTP Interception

Same as the HTTP interception technology of Ruijie First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of Ruijie First-Generation Web Authentication.

Working Principle

The networking topology of WiFiDog Web authentication is the same as shown in Figure 1-1.

Roles involved in WiFiDog Web authentication:

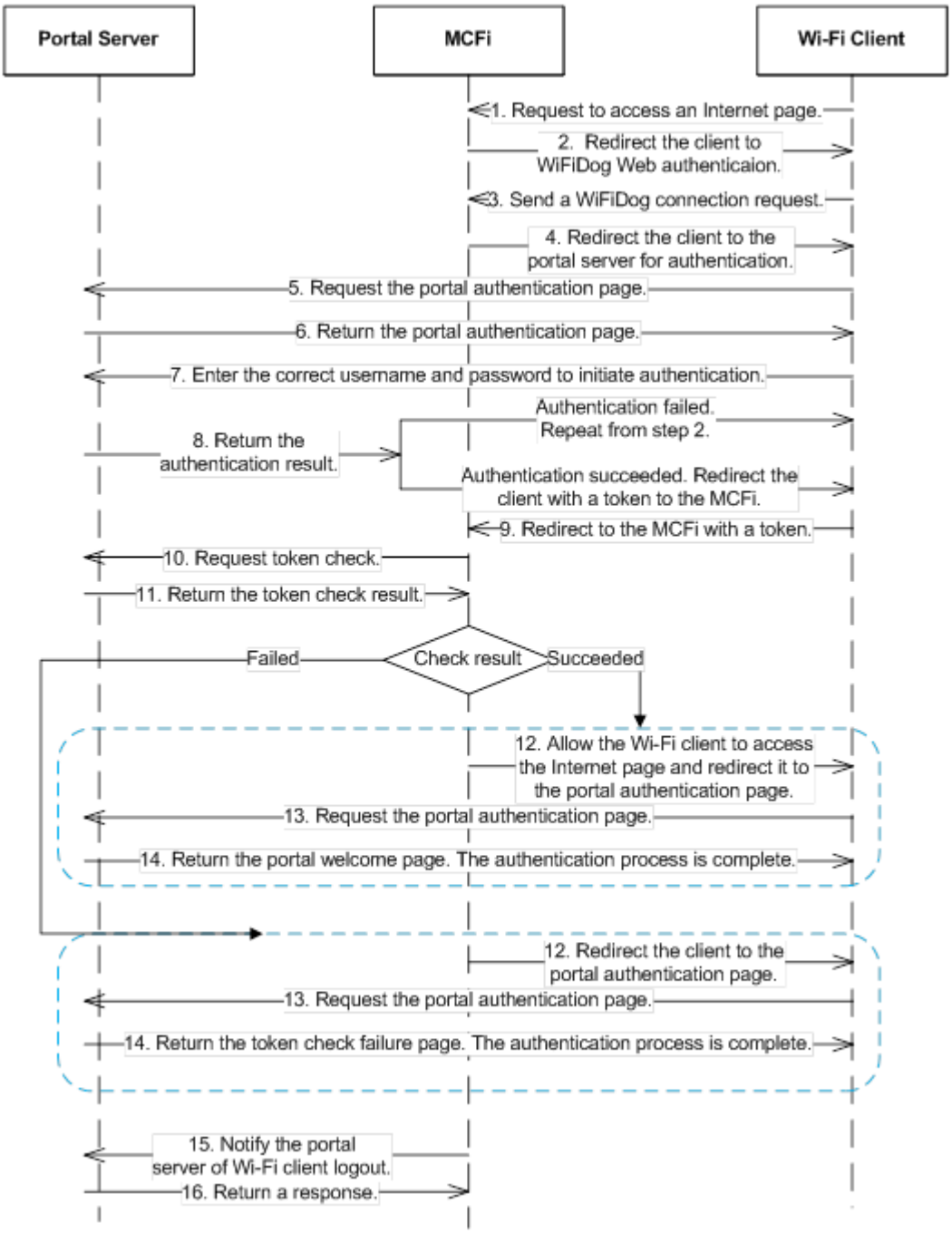
1. Authentication client: Is usually a browser running HTTP protocols. It sends HTTP requests for accessing the Internet.
2. NAS: Is an access-layer device in a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with Web authentication. The NAS controls users' Internet access permissions, receives the token check requests or Internet access requests from authentication clients, and initiates identity check to the portal server.
3. Portal server: Provides a Web page for Web authentication and related operations. The portal server receives the HTTP-based authentication requests from authentication clients and extracts account information from the requests. When authentication is complete in the background, the authentication clients forward the authentication results to the NAS. The NAS redirects the authentication clients to a Webpage provided by the portal server.

4. Authentication server: Provides the authentication service. The authentication server negotiates with the portal server to determine the protocol (for example, RADIUS) used by authentication.

Main process of WiFiDog Web authentication:

1. Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Thereafter, an authentication page is displayed on the browser.
2. During authentication, the client enters information, for example, username, password, and verification code, on the Webauth URL to interact with the portal server.
3. The portal server checks the validity of the client information in the background. If authentication fails, the portal server displays the failed authentication result to the client on a Web page. If authentication is successful, the portal server redirects the client to the NAS.
4. After receiving a request from the client, the NAS initiates check to the portal server. The NAS redirects the client to a Webpage provided by the portal server based on the check result.

Figure 1-4 Flowchart of WiFiDog Web Authentication



Client logout process:

There are two scenarios of client logout. One scenario is detected by the NAS that a client gets offline for the maximum online time is out, the upper traffic limit is reached, or the link is disconnected. The other scenario is detected by the portal server that a client logs out by clicking the **Logout** button on the logout page.

1. When a client clicks the **Logout** button, a logout request is sent to the portal server and NAS. (The logout request to the portal server and NAS may not be simultaneous, depending on the capability of the portal server.)

2. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.

Related Configuration

Configuring a WiFiDog Webauth Template

By default, the WiFiDog Webauth template is not configured.

Run the **web-auth template** {**wifidog** |*template-name* **wifidog** } command in global configuration mode to create a WiFiDog Webauth template.

The template is used to implement Web authentication.

Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** { *ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the Webauth URL of the Portal Server

By default, the Webauth URL of the portal server is not configured.

Run the **url** { *url-string* } command in template configuration mode to configure the Webauth URL of the portal server.

The URL to which clients are redirected is the address of the Webauth URL provided by the portal server.

Configuring the IP Address of the NAS

By default, the IP address of the NAS is not configured.

Run the **nas-ip** { *ip-address*} command in template configuration mode to configure the IP address of the NAS.

Ensure that the configured IP address is accessible by clients.

Configuring the Gateway ID

By default, the gateway ID is set to the serial number of the device. It is mandatory in hot backup and VAC scenarios. It can be set to the MAC address of a device.

Run the **gateway-id** *{ string }* command in template configuration mode to configure the gateway ID.

This parameter is carried in the WiFiDog packets and provided for the interconnected third-party portal.

Enabling WiFiDog Web Authentication

By default, WiFiDog Web authentication is disabled.

Run the **web-auth enable** { **eportalv2 |** *template-name* **v2** } command in interface configuration mode to enable Web authentication on the client-connected port.

After WiFiDog Web authentication is enabled, the unauthenticated clients connecting to a port will be redirected to the Webauth URL.

1.3.7. WeChat Web Authentication

HTTP Interception

Same as the HTTP interception technology of Ruijie First-Generation Web Authentication.

HTTP Redirection

Same as the HTTP redirection technology of Ruijie First-Generation Web Authentication.

Working Principle

The networking topology of WeChat Web authentication is the same as shown in Figure 1-1.

Roles involved in WeChat Web authentication:

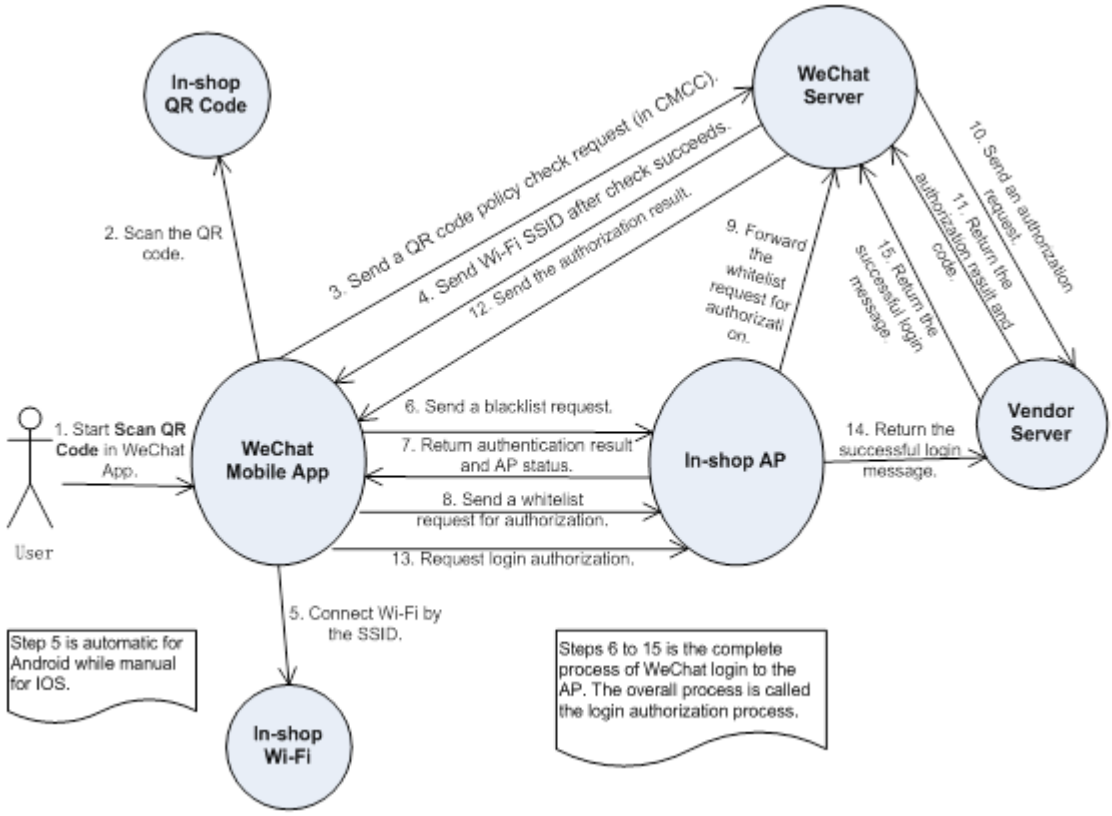
1. User: Is who sets up a Wi-Fi connection through WeChat to access the Internet.
2. In-shop AP: Is a fat AP or a fit AP.
3. Authentication server: Is a portal server or other authentication server like Marketing Cloud Platform (MCP), Wireless Marketing Cloud (WMC), or a third-party server.
4. WeChat server: Is a WeChat background server.

Process of scanning quick response (QR) codes by WeChat for authentication:

1. A user initiates a Wi-Fi connection request by scanning the QR code through WeChat.
2. The WeChat App identifies the QR code and calls the WeChat server (through the GSM by the mobile phone.)
3. The WeChat server checks the connection request based on the QR code policy.
4. The WeChat server returns an SSID to the WeChat user for its connection.
5. The WeChat user sends a connection request to the AP.
6. After connecting to the AP, the WeChat user sends a blacklist request, with the requested address being http://10.1.0.6/redirect. The request aims to inform the AP that the request is sent by a WeChat client.
7. After receiving the blacklist request, the AP sends a 302 redirection request, in which the auth parameter carries the MAC addresses of the mobile phone and AP in encryption mode.
8. After receiving the auth parameters, the WeChat client sends the WeChat server a whitelist request carrying the auth parameters for Wi-Fi connection authorization. Before that, the IP address of the WeChat server must be added to the whitelist of the AP to enable the AP to permit the authentication request to pass before the authentication on the AP is complete.
9. The AP determines that the requested IP address is in the whitelist and permits the whitelist request to pass to the WeChat server.
10. The WeChat server sends an HTTP-based authorization request to the device vendor server. The request maps interface 8. (Interface 13 must be called to set the device vendor server URL and token parameter in advance.)
11. The device vendor server implements authorization according to the authorization request and returns an authentication address and parameter (which maps the login parameter on interface 8).

12. The WeChat server returns the authentication address and parameter to the WeChat client.
13. The WeChat client requests the authentication address (by sending a login request).
14. The AP or device vendor server implements Internet access authentication. The AP permits the MAC address of the mobile phone to pass, and the device vendor server calls interface 7 to notify the WeChat server of successful Internet access (see step 15 in Figure 1-5). The AP returns a 302 redirection packet carrying the res=success parameter to the WeChat client. The WeChat client determines that Internet access authorization is successful based on this parameter. A page indicating that a Wi-Fi connection is set up successfully is displayed on the WeChat client.

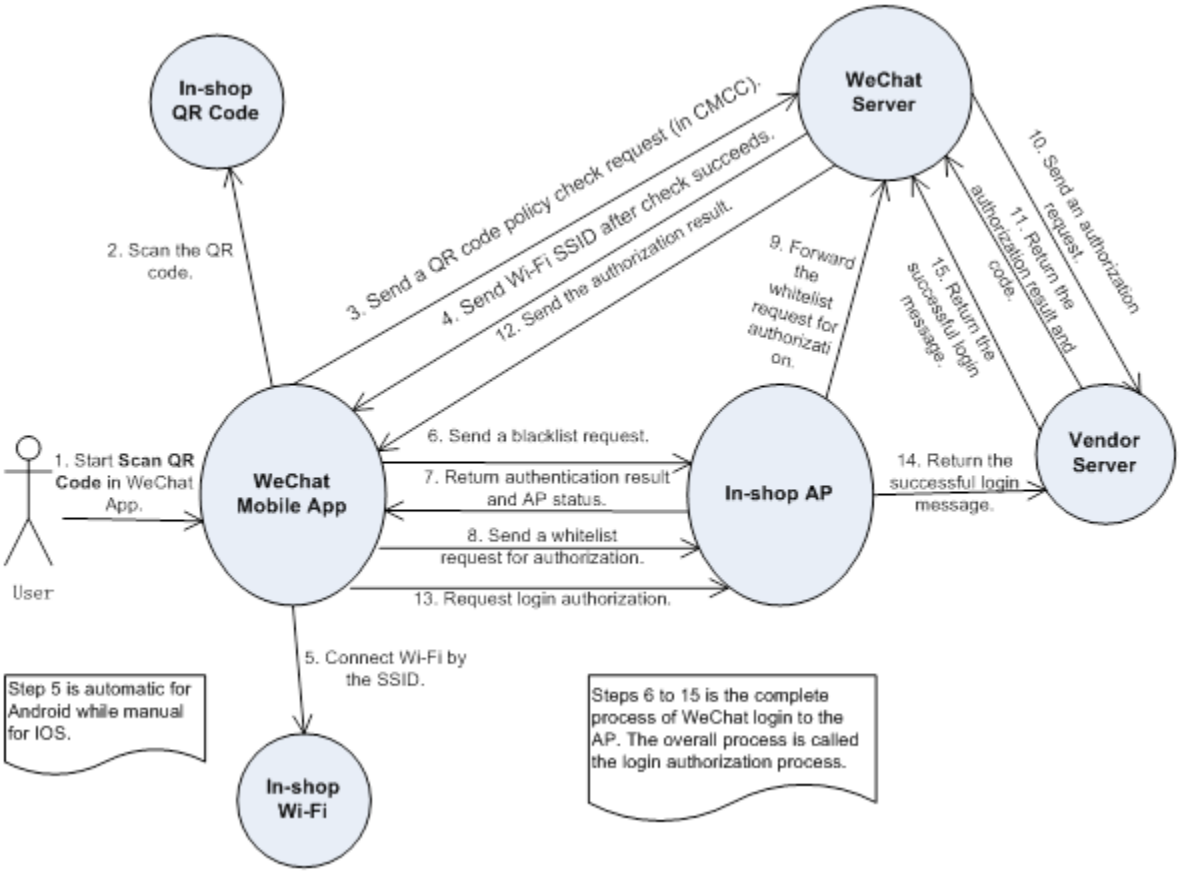
Figure 1-5 QR Code Scan Process in WeChat-Based Wi-Fi Connection Authentication



Process of the Internet access of multiple mobile devices by scanning dynamic QR codes on a PC:

A user starts a PC to set up a Wi-Fi connection and chooses to connect to an SSID (steps 1 and 2). When the user opens the browser and accesses a website, the browser sends a network request (step 3). The AP returns a 302 packet to display a portal authentication page on the browser. To enable a mobile phone to connect to the Internet by scanning a QR code displayed on the PC, the AP sends a request to the device vendor server (step 4), which calls interface 2 of the WeChat server to obtain the URL of the QR code photo (step 5). The WeChat server returns the URL of the QR code photo to the device vendor server (step 6), which then sends the URL to the AP (step 7). The AP sends the browser a 302 packet carrying the URL, which will be embedded into the portal authentication page. The mobile phone can scan the QR code (step 10) and connect to the Internet based on the normal access process.

Figure 1-6 Process Where Multiple Mobile Devices Access the Internet by Scanning Dynamic QR Codes on a PC



The NAS detects logout when a user's time is out, the data quota is reached, or the link is disconnected.

1. The NAS gets a client offline with traffic lower than the threshold based on the parameters of user online traffic detection.
2. The link disconnection duration depends on the parameters of anti-jitter configuration.

Related Configuration

↘ Configuring a WeChat Webauth Template

By default, the WeChat Webauth template is not configured.

Run the **web-auth template** {**wechat** |*template-name* **wechat** } command in global configuration mode to create a WeChat Webauth template.

The template is used to implement Web authentication.

↘ Configuring the IP Address of the Portal Server

By default, the IP address of the portal server is not configured.

Run the **ip** {*ip-address* } command in template configuration mode to configure the IP address of the portal server.

Any request packets to access the portal server will be filtered and rate-limited by the NAS.

Configuring the WeChat Webauth URL

By default, no WeChat Webauth URL is configured.

Run the **service-url** {*url-string* } command in template configuration mode to configure the WeChat Webauth URL.

The URL address is used for the communication between the NAS and portal server.

Configuring the Authentication Page Address for the Portal Server

By default, the authentication page address of the Portal server is not configured.

Run the **url** { *url-string* } command to configure the authentication page address for the Portal server in template configuration mode.

The address is accessed by a terminal after redirection. The function is optional for devices of version 11.1(5)B9 and the default configuration can be used.

Configuring the IP Address of the NAS

By default, the IP address of the NAS is not configured.

Run the **nas-ip** command in template configuration mode to configure the IP address of the NAS.

Ensure that the configured IP address is accessible by users and must not be configured as a straight-through address.

Configuring the Portal Communication Key

By default, no encryption key is configured.

Run the **key** {*key-string*} command in template configuration mode to configure an encryption key used for communicating with the portal server.

The encryption key is used to encrypt user authentication information and must be consistent with the key configured on the portal server.

Configuring NAS ID

By default, the NAS ID is the MAC address of the device.

You have to configure the NAS ID in scenarios of hot backup or VAC.

In AC configuration mode, run **nas-id** { *nas-id-string* } the command to configure the NAS ID.

Enabling Web Authentication

By default, Web authentication is disabled.

Run the **web-auth portal** { **wechat |** *template-name* **wechat** } command in WLAN security configuration mode and **webauth** command to enable Web authentication control on the STA-connected port.

After Web authentication is enabled, the unauthenticated STAs connecting to the port will be redirected to a one-click Internet access page provided by the portal server, and the unauthenticated PCs connecting to the port will be redirected to a QR code page.

Enabling the Single Escape Function

By default, the escape function is disabled. And this function is supported only in the version 11.1(5)B23.

Run the **escape user-try-auth** *counts* **online-time** *minutes* command in template configuration mode to enable the escape function.

With the escape function, if the number of authorization requests that an STA sends exceeds the configured value (specified by the **escape user-try-auth** *counts* parameter), but no successful authentication is achieved, then the NAS lets the STA escape and permits the corresponding entry to pass. The escape duration is specified by the **online-time** *minutes* parameter.

Enabling the Escape Function

By default, the escape function is disabled.

Run the **web-auth wechat-escape interval** *minutes* command in global configuration mode or WLAN security configuration mode to enable the escape function. Configuration in WLAN security configuration mode takes priority over that in global configuration mode. If this command is run in global configuration mode but not in WLAN security configuration mode, then the configuration in global configuration takes effect.

After configuration, if the server is unreachable or the server allows STAs to escape, later access STAs are exempted from authentication and permitted to escape. The escape duration is specified by the **interval** *minutes* parameter.

To cancel escape, run the **web-auth wechat-escape recover** command in global configuration mode.

Configuring Server Detection

By default, server detection is disabled.

Run the **web-auth wechat-check interval** *minutes* command in global configuration mode to enable server detection.

After the function is configured, the device detects the server. If it fails to receive the serve response or the response is unavailable within a certain interval (specified by **interval** *minutes*) and the collective escape function is configured on the device, all users who gain access later are permitted to pass without authentication.

To cancel server detection, run the **no web-auth wechat-check** command in global configuration mode.

1.4. Configuration

Configuration	Description and Command	
Configuring Ruijie First-Generation Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie First-Generation Web Authentication.	
	web-auth template eportalv1	Configures the first-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.

Configuration	Description and Command	
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	snmp-server community { *community-string* } **rw**	Configures the SNMP-server community string.
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	Configures the SNMP-server host.
	snmp-server enable traps web-auth	Enables the SNMP-server Trap/Inform function.
	web-auth enable	Enables Ruijie First-Generation Web Authentication on an interface.
Configuring Ruijie Second-Generation Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie Second-Generation Web Authentication.	
	aaa new-model	Enables AAA.
	radius-server host {*ip-address*}[**auth-port** *port-number*] [**acct-port** *port-number*] **key** {*string*}	Configures the RADIUS-server host and communication key.
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Web authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Web Accounting. (RADIUS accounting is implemented.)
	web-auth template{**eportalv2 |***portal-name***v2**}	Configures a second-generation Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	web-auth portal key { *key-string* }	Configures the Webauth communication key.
	web-auth enable{ **eportalv2 |** *template-name* }	Enables Ruijie Second-Generation Web Authentication on an interface.
Configuring Ruijie iPortal Web Authentication	⚠ (Mandatory) It is used to set the basic parameters of Ruijie iPortal Web authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	Configures the RADIUS-server host and communication key.

Configuration	Description and Command	
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal Web Authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal Web Accounting. (RADIUS accounting is implemented.)
	web-auth template iportal	Configures the iPortal Web-auth template.
	web-auth enable iportal	Enables Ruijie iPortal Web Authentication on an interface.
Configuring MAC Address-Based SMS Authentication	(Mandatory) It is used to set the basic parameters of MAC address-based SMS authentication.	
	aaa new-model	Enables AAA.
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	Configures the RADIUS-server host and communication key.
	web-auth template eportalv2	Configures a second-generation Webauth template.
	web-auth sms-flow interval *interval* **threshold** *flows*	Configures the detection interval and traffic threshold for MAC address-based SMS authentication.
	web-auth bind-portal *string* **[type { group-spec | local-spec}]**	Configures the portal server bound for MAC address-based SMS authentication.
	web-auth winterface *string*	Sets the **winterface** field in the redirected URL.
	web-auth wlan-ac-ip *ipv4*	Sets the **ACIP** field in the redirection URL.
Configuring WiFiDog Authentication	(Mandatory) It is used to set the basic parameters of WiFiDog authentication.	
	web-auth template wifidog	Configures a WiFiDog authentication template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	url { *url-string* }	Configures the Webauth URL of the portal server.
	nas-ip { *ip-address* }	Configures the IP address of the NAS.
	web-auth portal wifidog	Specifies a WiFiDog authentication template.
	webauth	Enables Web authentication.

Configuration	Description and Command	
Configuring WeChat Web Authentication	(Mandatory) It is used to set the basic parameters of WeChat authentication.	
	web-auth template { **wechat	(***portal-name* **wechat** *)*}	Configures a WeChat Webauth template.
	ip {*ip-address* }	Configures the IP address of the portal server.
	service-url { *url-string* }	Configures the WeChat Webauth URL.
	key { *key-string* }	Configures the portal communication key.
	web-auth portal wechat	Specifies a WeChat Webauth template.
	webauth	Enables Web authentication.
Specifying an Authentication Method List	(Optional) It is used to specify an AAA authentication method list in template configuration mode. The name of the method list must be correctly specified.	
	authentication { *mlist-name* }	Specifies an AAA authentication method list(only for Ruijie Second-Generation Web Authentication and Ruijie iPortal Web Authentication.)
Specifying an Accounting Method List	(Optional) It is used to specify an AAA accounting method in template configuration mode. The name of the method list must be correctly specified.	
	accounting { *mlist-name* }	Specifies an AAA accounting method list(only for Ruijie Second-Generation Web Authentication and Ruijie iPortal Web Authentication.)
Configuring the Communication Port of the Portal Server	(Optional) It is used to specify the UDP port of the portal server in template configuration mode. The configured port number must be consistent with that on the RADIUS server.	
	port { *port-num* }	Configures the communication port of the portal server.
Specifying the Webauth Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	
	**bindmode {ip-mac-mode	ip-only-mode}**	Specifies the template binding mode.
Customizing a Page Suite	(Optional) It is used to configure the page suite used by Ruijie iPortal Web Authentication for a template.	
	page-suite *file-name*	Customizes a page suite for Ruijie iPortal Web Authentication.
Configuring an Advertisement URL	(Optional) It is used to configure an iPortal Webauth advertisement URL in template configuration mode.	

Configuration	Description and Command	
	popup *url*	Configures an iPortal Webauth advertisement URL.
Specifying the Advertisement Mode	(Optional) It is used to specify the iPortal Webauth advertisement mode in template configuration mode.	
	popup-mode [login-popup | online-popup]	Specifies the iPortal Webauth advertisement mode.
Configuring the Format of the Webauth URL	(Optional) It is used to configure the redirection URL format for a template.	
	fmt custom	Configures the format of the Webauth URL.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that the packets on the specified port can be redirected when interception is enabled.	
	http redirect port { *port-num* }	Configures the redirection TCP port.
Configuring Rate Limit Webauth Logging	(Optional) It is used to configure the syslog function in Web authentication.	
	web-auth logging enable {*num* }	Configures the rate limit Webauth logging.
Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients	(Optional) It is used to adjust the HTTP session limit. The limit value needs to be increased when there are many sessions in the background.	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	Configures the maximum number of HTTP sessions for unauthenticated clients.
Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout period for redirection connections. The timeout needs to be increased to complete redirection when the network condition is bad.	
	http redirect timeout{ *seconds* }	Configures the HTTP redirection timeout.
Configuring the Straight-Through ARP Resource Range	(Optional) It is used to permit the ARP of the specified addresses to pass. The gateway ARP must be permitted to pass when ARP check is enabled.	
	http redirect direct-arp { *ip-address* [*ip-mask*] }	Configures the straight-through ARP resource.
Configuring an Authentication-Exempted Address Range	(Optional) It is used to exempt clients from authentication when accessing the Internet.	
	web-auth direct-host { *ip-address* [i*p-mask*] [**arp**] } [**port** *interface-name* | *mac-address* }	Configures the range of the IP or MAC addresses of clients free from authentication.
Configuring the Interval for Updating Online User Information	(Optional) It is used to configure the interval for updating online user information.	
	web-auth update-interval *{ seconds }*	Configures the interval for updating online user information.

Configuration	Description and Command	
Configuring Portal Detection	(Optional) It is used to detect the availability of the portal server. If it is not available, the services are switched to the standby portal server. This function must be used together with portal standby function.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**	Configures the portal server detection interval, timeout period, and timeout retransmission times.
	web-auth ping [**interval** *minutes*] [**retry** *times*]	Configures the ping detection interval and timeout retransmission times.
Configuring Portal Escape	(Optional) It is used to allow new clients to access the Internet without authentication when the portal server is not available.	
	web-auth portal-escape	Configures portal escape.
Enabling DHCP Address Check	(Optional) It is used to check whether the IP address of a client is allocated by the DHCP server. If not, the client's authentication request is denied.	
	web-auth dhcp-check	Checks whether the IP address of a client is assigned by the DHCP server.
Disabling Link Detection	(Optional) It is used for jitter-off purposes to prevent the deletion of a client's Web authentication entry when the link of the client is disconnected, so that the client can access the Internet again without authentication.	
	no web-auth sta-leave detection	Disables link detection.
Disabling Portal Extension	(Optional) It is used to disable portal extension in order to interwork with CMCC standard portal server. Portal extension must be enabled for interworking with Ruijie portal server software.	
	no web-auth portal extension	Disables portal extension.
Configuring a Whitelist and Blacklist	(Optional) It is used to configure a blacklist to prevent authenticated clients from accessing some network resources, and a whitelist to allow unauthenticated clients to access some network resources.	
	web-auth acl{black-ip *ip***|black-port** *port***|black-url** *name***|white-url** *name***}**	Configures a whitelist and blacklist.
Configuring Jitter-off Accounting	(Optional) It is used to configure whether the jitter-off duration is included into the online duration, in order to improve accounting precision. The jitter-off duration depends on the jitter-off configuration of a specific product.	
	web-auth accounting jitter-off	Configures the jitter-off duration. (Use the **no** form of this command to disable this function.)

Configuration	Description and Command	
Configuring the Portal Communication Port	(Optional) It is used to configure the port (source port) used for the communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for the communication between the NAS and portal server.
Configuring a NDKEY-Compatible Webauth URL	(Optional) It is used to configure the Webauth URL used in Web authentication to support the Shanghai NDKEY system.	
	web-auth dkey-compatible url-parameter *string*	Configures a NDKEY-Compatibility compatible between the Shanghai NDKEY system and redirection Webauth URL.
Enabling NAT for Ruijie iPortal Web Authentication	(Optional) It is used to configure Ruijie iPortal Web Authentication to support network address translation (NAT).	
	iportal nat enable	Enables NAT for Ruijie iPortal Web Authentication.
Configuring the iPortal HTTP Retransmission Times	(Optional) It is used to configure the iPortal HTTP retransmission times.	
	iportal retransmit *count*	Configures the iPortal HTTP retransmission times.
Configuring Service Selection in Ruijie iPortal Web Authentication	(Optional) It is used to configure the service type used by Ruijie iPortal Web Authentication.	
	iportal service [**internet** *internet-name*] [**local** *local-name*]	Configures the service type used by Ruijie iPortal Web Authentication.
Configuring the Accounting Method List of Web Authentication	(Optional) It is used to configure an accounting method based on the template.	
	web-auth accounting v2 { default | *name*}	Configures an accounting method based on the template.
Configuring a Web Authentication Method List	(Optional) It is used to configure an authentication method based on the template.	
	web-auth authentication v2 { **default |** *name*}	Configures an authentication method based on the template.
Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication	(Optional) It is used to enable the automatic display of a Web configuration page in iOS systems with wireless association.	
	http redirect adapter ios	Enables the automatic display of a Web configuration page in iOS systems with wireless association.

Configuration	Description and Command	
Configuring Online User Detection Under WLANSEC	⚠ (Optional) It is used to configure online user detection under WLANSEC.	
	web-auth offline-detect interval *interval* **flow** *thredshold*	Configures online user detection under WLANSEC.
Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol	⚠ (Optional) It is used to configure transparent transmission of the 0x05 attribute of the portal protocol.	
	web-auth portal-attribute [5 | textinfo]	Configures transparent transmission of the 0x05 attribute of the portal protocol.
Configuring Uniqueness Check of Portal Authentication Accounts	⚠ (Optional) It is used to configure uniqueness check of portal authentication accounts.	
	web-auth portal-valid unique-name	Configures uniqueness check of portal authentication accounts.
Enabling One-click Wireless Configuration via WiFiDog	⚠ (Optional) It is used to enable one-click wireless configuration via WiFiDog.	
	web-auth wifidog-template wlan-range portal-ip nas-ip url [perception]	Enables one-click wireless configuration via WiFiDog.
Enabling One-click Wireless Configuration via WeChat Connection to Wi-Fi	⚠ (Optional) It is used to enable one-click wireless configuration via Wechat connection to WiFi.	
	web-auth wechat-template wlan-range portal-ip nas-ip [ios-adapter | perception]	Enables one-click wireless configuration via WeChat connection to WiFi.

1.4.1. Configuring Ruijie First-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- (Mandatory)To enable Web authentication successfully, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Setting the SNMP Parameters Between the NAS and Portal Server

- (Mandatory) To enable Web authentication successfully, you must set the SNMP network management parameters used for the communication between the NAS and portal server.
- The NAS or convergence device and portal server jointly manage authenticated clients through SNMP/MIB. A table of authenticated clients is managed by MIB on the NAS. The portal server is able to access the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or convergence device will inform the portal server by Webauth Inform packets.

Enabling Ruijie First-Generation Web Authentication on an Interface

- Mandatory.
- When Ruijie First-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring the First-Generation Webauth Template

Command	**web-auth template eportalv1**
Parameter Description	N/A
Command	Global configuration mode

Mode	
Usage Guide	**eportalv1** is the default template of Ruijie First-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** {*ip-address*}
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** {*url-string*}
Parameter Description	*url-string*: Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt** { **ace	ruijie** }
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	ACE association is supported when **fmt** is set to **ace**.

Specifying the Webauth Binding Mode

Command	**bindmode** { **ip-mac-mode	ip-only-mode** }
Parameter Description	Indicates the Webauth binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Specifying the Redirection Method

Command	**redirect** { **http	js** }
Parameter Description	Indicates the encapsulation format of redirected packets.
Command	Webauth template configuration mode

Mode	
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

Command	**web-auth portal key** {*key-string*}
Parameter Description	*key-string:* Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the SNMP-Server Community String

Command	**snmp-server community** {*community-string*}**rw**
Parameter Description	*community-string*: Indicates the community string. **rw**: Must be set to **rw** to support the read and write operations as the Set operation on MIB is required.
Command Mode	Global configuration mode
Usage Guide	The SNMP-server community string is used by the portal server to manage the online clients on the NAS or convergence device.

Configuring the SNMP-Server Host

Command	**snmp-server host** {*ip-address*} **inform version 2c** {*community-string*} **web-auth**
Parameter Description	*ip-address*: Indicates the IP address of the SNMP-server host, that is, the portal server. *community-string*: Configures the community string used to send an SNMP Inform message.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP-server host to receive Webauth messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or convergence device will send a message to the portal server when a client logs out. The message type is set to Inform instead of Trap to avoid message loss. **version 2c**: Indicates SNMPv2 for SNMP Inform is not supported in all SNMP versions excluding SNMPv1. **web-auth**: Indicates the preceding parameters to be used for Web authentication. For details regarding SNMP configuration and others, see the *Configuring SNMP*. The SNMP parameter **version 2c**listed here is aimed at SNMPv2. SNMPv3 is recommended if higher security is required for the SNMP communication between the NAS and portal server. To use SNMPv3, change **SNMP Community** to **SNMP User**, **version 2c** to **SNMPv3**, and set SNMPv3-related security parameters. For details, see the *Configuring SNMP*.

Enabling the Webauth Trap/Inform Function

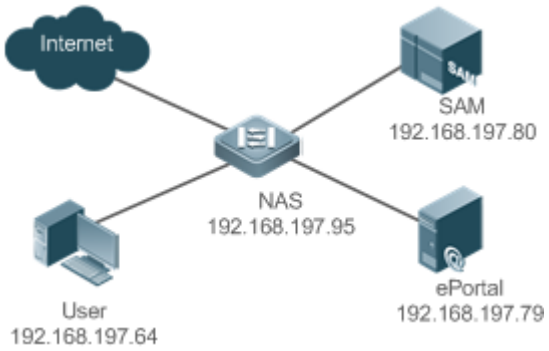
Command	**snmp-server enable traps web-auth**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or convergence device to send Webauth Trap and Inform messages externally. web-auth: Indicates Web authentication messages.

Enabling Ruijie First-Generation Web Authentication on an Interface

Command	**web-auth enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie First-Generation Web Authentication

Scenario **Figure 1-7**	
Configuration Steps	● On the NAS, configure the IP address of the ePortal server and the key (ruijie) used for communicating with the ePortal server. ● Configure the Webauth URL on the NAS. ● Set the SNMP network management parameters (community string: public) used for the communication between the NAS and ePortal server. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	`Ruijie# config` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#web-auth template eportalv1`

	Ruijie(config.tmplt.eportalv1)#ip 192.168.197.79 Ruijie(config.tmplt.eportalv1)#exit Ruijie(config)# web-auth portal key ruijie
	Ruijie(config)# web-auth template eportalv1 Ruijie(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp Ruijie(config.tmplt.eportalv1)#exit
	Ruijie(config)# snmp-server community public rw Ruijie(config)# snmp-server enable traps web-auth Ruijie(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth Ruijie(config)# exit
	Ruijie(config)# interface range GigabitEthernet 0/2-3 Ruijie(config-if-range)# web-auth enable Ruijie(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.
	Ruijie(config)#show running-config … snmp-server host 192.168.197.79 inform version 2c public web-auth snmp-server enable traps web-auth snmp-server community public rw … web-auth template eportalv1 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key ruijie … interface GigabitEthernet 0/2 web-auth enable ! interface GigabitEthernet 0/3

	web-auth enable
	Ruijie#show web-auth control Port Control Server Name Online User Count ---------- -------- ---------- ---------- ... GigabitEthernet 0/20n eportalv1 0 GigabitEthernet 0/30n eportalv1 0 ...
	Ruijie#show web-auth template Webauth Template Settings: ---------- Name: eportalv1 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v1 .....

Common Errors

- The SNMP parameters used for the communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- Specify the IP-MAC binding mode to deploy Web authentication on layer-3 networks, causing authentication failures.
- When Web authentication is used in conjunction with VRRP, run the snmp-server trap-source ip command to specify the VRRP address; otherwise, the portal server cannot process Trap packets correctly.

1.4.2. Configuring Ruijie Second-Generation Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. IPv6 is supported.

Notes

- Ruijie Second-Generation Web Authentication complies with the CMCC WLAN Service Portal Specification. Furthermore, it is extended to support Ruijie portal server. Perform compatible configuration based on the server performance in actual deployment. For details, see the subsequent chapter.

- When you configure the URL of the second-generation portal server, if the URL contains an IPv6 address, enclose it with a pair of square brackets, for example, http://[2001::1]/index.jsp.
- The cmcc-normal and cmcc-ext1 parameters in the fmt command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid.

Configuration Steps

Enabling AAA

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie Second-Generation Web Authentication.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA method list for Web accounting.
- An accounting method list is used to associate an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the Portal Server

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.

- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Configuring the Portal Server in Global or Interface Configuration Mode

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must specify the use of the second generation portal server in global or interface configuration mode.
- The NAS first selects the portal server in interface configuration mode. If such a portal server does not exist, the NAS selects the portal server in global configuration mode. If such a portal server does not exist, eportalv1 is used by default. The NAS redirects users to the selected portal server.

Enabling Ruijie Second-Generation Web Authentication on an Interface

- Mandatory.
- When Ruijie Second-Generation Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** {*ip-address*} [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** {*string*}
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

Command	**web-auth template**{**eportalv2 |** *portal-name* **v2**}
Parameter Description	*portal-name*: Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of Ruijie Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* | *ipv6-address*}
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** { *url-string* }
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode

Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt** {**cmcc-ext1	cmcc-ext2	cmcc-mtx	cmcc-normal	ct-jc	cucc| ruijie	custom**}
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	The **cmcc-normal** and **cmcc-ext1** parameters in the **fmt** command support only IPv4. If IPv6 is used, the configuration of the portal server is invalid. The **cmcc-ext2** is supported for Liaoning CMCC. When **fmt** is set to **cmcc-mtx**, the URL format of mobile AC vendors is supported. The **ct-jc** format is supported for Chine Telecom. The **cucc** format is supported for Shandong China Telecom. The **custom** format is defined by users.

Specifying the Encapsulation Format of the Webauth URL

Command	**redirect { http	js }**
Parameter Description	Indicates the encapsulation format of redirected packets.
Command Mode	Webauth template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Webauth Communication Key

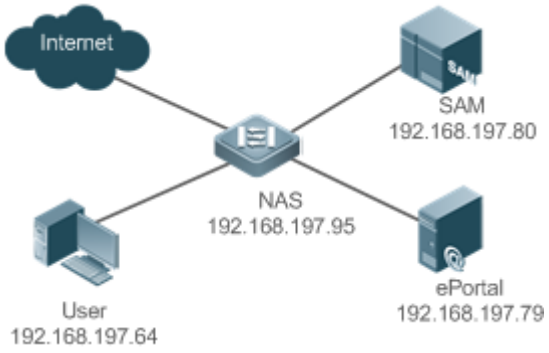
Command	**web-auth portal key** { *key-string* }
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Ruijie Second-Generation Web Authentication on an Interface

Command	**web-auth enable** {**eportalv2 |** *template-name*}
Parameter Description	Indicates a Webauth template.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie Second-Generation Web Authentication

Scenario **Figure 1-8**	
Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA method lists for Web authentication and accounting on the NAS. ● Configure the IP address of the portal server and the Webauth communication key (ruijie) used for communicating with the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure Ruijie Second-Generation Web Authentication in global configuration mode on the NAS. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	`Ruijie#configure` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#aaa new-model`
	`Ruijie(config)#radius-server host 192.168.197.79 key ruijie`
	`Ruijie(config)#aaa authentication web-auth default group radius` `Ruijie(config)#aaa accounting network default start-stop group radius`
	`Ruijie(config)#web-auth template eportalv2` `Ruijie(config.tmplt.eportalv2)#ip 192.168.197.79` `Ruijie(config.tmplt.eportalv2)#exit` `Ruijie(config)#web-auth portal key ruijie`
	`Ruijie(config)# web-auth template eportalv2` `Ruijie(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp` `Ruijie(config.tmplt.eportalv2)#exit`
	`Ruijie(config)# interface range GigabitEthernet 0/2-3` `Ruijie(config-if-range)# web-auth enable eportalv2`

	Ruijie(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.
	Ruijie(config)#show running-config … aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius … radius-server host 192.168.197.79 key ruijie … web-auth template eportalv2 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp ! web-auth portal key ruijie … interface GigabitEthernet 0/2 web-auth enable eportalv2 ! interface GigabitEthernet 0/3 web-auth enable eportalv2
	Ruijie#show web-auth control Port Control Server Name Online User Count ------------------------ -------- -------------------- ----------------- … GigabitEthernet 0/2 On eportalv2 0 GigabitEthernet 0/3 On eportalv2 0 …
	Ruijie#show web-auth template Webauth Template Settings:

```
-----------------------------------------------------------

  Name:      eportalv2

  Url:       http://17.17.1.21:8080/eportal/index.jsp

  Ip:        17.17.1.21

  BindMode:  ip-mac-mode

  Type:      v2

  Port:      50100

State:     Active

  Acctmlist: default

  Authmlist: default

...
```

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the *CMCC WLAN Service Portal Specification*, causing compatibility failure.

1.4.3. Configuring Ruijie iPortal Web Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication. No external portal server is required.

Notes

- Some devices, such asAP110, do not have a built-in page suite. You need to import a page suite before use. For details about the page suite support on a product, see the corresponding product description.
- Ruijie iPortal Web Authentication is configured on EG devices in global configuration mode.
- To configure a customized page suite, the configuration must comply with the relevant specification.

Configuration Steps

↘ Enabling AAA

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must enable AAA.
- The iPortal NAS is responsible for initiating authentication to the portal server through AAA in Ruijie iPortal Web authentication.

↘ Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable Ruijie iPortal Web Authentication, you must configure the RADIUS-server host.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Configuring an AAA Method List for Ruijie iPortal Web Authentication

- (Mandatory) To enable Ruijie iPortal Web Authentication, you must configure an AAA method list for Ruijie iPortal Web Authentication.
- An AAA authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the method list.

Configuring an AAA Method List for Ruijie iPortal Web Accounting

- (Optional) Some servers require that authentication and accounting be enabled. Configure Web accounting based on the characteristics of the server in use.
- An AAA accounting method list associates an accounting method and server. In Web authentication, accounting is implemented to record client fees.

Configuring the iPortal Webauth Template

- Mandatory.
- If any non-default authentication and accounting method lists are configured, you need to specify the name of a method list in template configuration mode; otherwise, the default method list is used.

Enabling Ruijie iPortal Web Authentication Globally or on an Interface

- Mandatory.

Verification

- Check whether unauthenticated clients are redirected to the Webauth URL to perform authentication, and the Webauth URL displayed is that in the page suite.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Enabling AAA

Command	aaa new-model
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

Command	**radius-server host** { *ip-address* } [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS-server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Ruijie iPortal Web Authentication

Command	**aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring an AAA Method List for Web Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	The specified AAA method should exist in the AAA configuration.

Configuring the iPortal Webauth Template

Command	**web-auth template iportal**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Pre-login Advertisement Mode

Command	**login-popup**{ *url-string* }
Parameter Description	Indicates the advertisement URL.
Command	Webauth template configuration mode

Mode	
Usage Guide	The URL starts with **http://** or **https://**.

Specifying the Post-login Advertisement Mode

Command	**online-popup** {url-string}
Parameter Description	Indicates the advertisement URL.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Customizing a Page Suite

Command	**page-suit**{*filename*}
Parameter Description	Indicates the file name of a page suite.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the iPortal Advertisement Interval

Command	**time-interval** {*hour*}
Parameter Description	Indicates the advertisement interval.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Enabling Ruijie iPortal Web Authentication on an Interface

Command	**web-auth enable iportal**
Parameter Description	Indicates the customized template name.
Command Mode	Interface configuration mode or global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie iPortal Web Authentication

Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA authentication and accounting method lists on the NAS.

	● Configure the global use of the iPortal server on the NAS. ● Enable Web authentication on ports GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS.
	Ruijie#configure Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#aaa new-model
	Ruijie(config)#radius-server host 192.168.197.79 key ruijie
	Ruijie(config)#aaa authentication iportal default group radius Ruijie(config)#aaa accounting network default start-stop group radius
	Ruijie(config)#web-auth template iportal
	Ruijie(config.tmplt.iportal)#exit
	Ruijie(config)# interface range GigabitEthernet 0/2-3 Ruijie(config-if-range)# web-auth enable iportal Ruijie(config-if-range)# exit
Verification	● Check whether Ruijie iPortal Web Authentication is configured successfully.
	Ruijie(config)#show running-config … aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius … radius-server host 192.168.197.79 key ruijie … web-auth template iportal ! … interface GigabitEthernet 0/2 web-auth enable iportal ! interface GigabitEthernet 0/3 web-auth enable iportal

	Ruijie#show web-auth control Port Control Server Name Online User Count ------------------------ -------- -------------------- ----------------- ... GigabitEthernet 0/2 On iportal 0 GigabitEthernet 0/3 On iportal 0 ...
	Ruijie#show web-auth template Webauth Template Settings: -- Name: iportal Page-suit: default BindMode: ip-mac-mode Type: Intral Portal Advertising: null Advertising mode : online-popup Acctmlist: default Authmlist: default ...

Common Errors

- The preparation of a page suite does not comply with the relevant specification.
- A page suite is specified, but is not downloaded to the flash memory or the specified directory.

1.4.4. Configuring WiFiDog Authentication

Configuration Effect

Redirect unauthenticated clients to the Webauth URL to perform authentication.

Notes

N/A

Configuration Steps

↘ Configuring the Portal Server

- (Mandatory) To enable Web authentication, you must configure and apply the portal server.
- When the NAS finds an unauthenticated client attempting to access network resources through HTTP, it redirects the client's access requests to the specified Webauth URL, where the client can initiate authentication to the portal server. The IP address of the portal server is configured as a network resource which clients can access without authentication. Unauthenticated clients can directly access this IP address through HTTP.

Configuring the IP Address of the NAS

- Mandatory.
- By default, the IP address of the NAS is not configured.
- Ensure that the configured IP address is accessible by clients.

Enabling Ruijie iPortal Web Authentication on an Interface

- Mandatory.
- When Ruijie iPortal Web Authentication is enabled in interface configuration mode, Web authentication is not enabled on any port by default. The users connecting to the port do not need to perform Web authentication.

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring a WiFiDog Webauth Template

Command	**web-auth template wifidog**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	**wifidog** means the default WiFiDog Webauth template.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** { *url-string* }

Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	The URL starts with **http://**.

Configuring the IP Address of the NAS

Command	**nas-ip** { *ip-address* }
Parameter Description	Indicates the IP address of the NAS.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured IP address is accessible by clients.

Configuring the Gateway ID

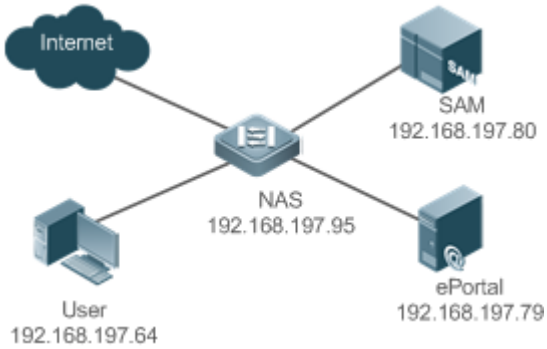
Command	**gateway-id** { *string* }
Parameter Description	*string*: Indicates the gateway ID used in WiFiDog. It is the serial number of the device by default.
Command Mode	Web authentication template configuration mode
Usage Guide	This parameter is carried in the WiFiDog packets and provided for the interconnected third-party portal. It is mandatory in hot backup and VAC scenarios.

Enabling WiFiDog Web Authentication on an Interface

Command	**web-auth enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuring WiFiDog Web Authentication

Scenario **Figure 1-9**	
Configuration Steps	● Configure the IP address of the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure the IP address used for external communication on the NAS. ● Enable WiFiDog Web authentication for WLAN10 on the NAS.
	Ruijie# config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#web-auth template wifidog Ruijie(config.tmplt.wifidog)#ip 192.168.197.79
	Ruijie(config.tmplt.wifidog)#url http://192.168.197.79/auth/wifidogAuth Ruijie(config.tmplt.wifidog)#nas-ip 192.168.197.95 Ruijie(config.tmplt.wifidog)#exit
	Ruijie(config)# wlansec 10
	Ruijie(config-wlansec)#web-auth portal wifidog Ruijie(config-if-range)# webauth Ruijie(config-if-range)# exit
Verification	● Check whether WiFiDog Web authentication is configured successfully.
	Ruijie(config)#show running-config … web-auth template wifidog ip 192.168.197.79 nas-ip 192.168.197.95 url http://192.168.197.79/auth/wifidogAuth

	... wlansec 10 web-auth portal wifidog webauth
	Ruijie#show web-auth control Port Control Server Name Online User Count ------------------------ -------- -------------------- ----------------- wlansec 10 On wifidog 0 ...
	Ruijie#show web-auth template Webauth Template Settings: -- Name: wifidog Type: wifidog Ip: 192.168.197.79 Url: http://192.168.197.79/auth/wifidogAuth NasIp: 192.168.197.95 .....

Common Errors

- The IP address of the NAS is not configured, causing a redirection failure.

1.4.5. Configuring MAC Address-Based SMS Authentication

Configuration Effect

Allow unauthenticated clients connected to WLAN to access network resources. When a user uses up the traffic during the specified time period, the NAS initiates a MAC address binding query to the bound portal server. If the user is bound with a MAC address, the portal server initiates an authentication request. If the STA is not bound with a MAC address, the STA needs to perform authentication on the portal server before accessing the Internet.

Notes

- MAC address-based SMS authentication is supported only on wireless devices.
- The configured URL of the portal server must adopt the **cmcc-ext1** format.

Configuration Steps

Enabling AAA

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie Second-Generation Web Authentication.

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can configure the AAA authentication and accounting method lists only after AAA is enabled.

Configuring the RADIUS-Server Host and Communication Key

- (Mandatory) To enable MAC address-based SMS authentication, you must configure the RADIUS server.
- Clients' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a client.

Command	**radius-server host** { *ip-address* } [**auth-port***port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server host. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812, and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure an AAA authentication method list on the AAA module.
- A Web authentication method list associates Web authentication requests with the RADIUS server. The NAS selects an authentication method and server based on the Web authentication method list.

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Indicates a method list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS authentication method.

Configuring an AAA Method List for Web Accounting

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure a network accounting method on the AAA module.
- A network accounting method is used to associate an accounting method and server. In Web authentication, accounting is implemented to record user information or fees.

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Indicates a method list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie Second-Generation Web Authentication adopts the RADIUS accounting method.

Configuring the Second-Generation Webauth Template

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure and apply the portal server.
- When the NAS or convergence device finds an unauthenticated client attempting to access network resources through HTTP, it redirects the access request to the specified Webauth URL, where the client can initiate authentication to the portal server. If the IP address of the portal server is configured as a free network resource, unauthenticated clients can directly visit this IP address through HTTP.

Command	**web-auth template** { **eportalv2 |** *portal-name* **v2**}
Parameter Description	Indicates the customized portal server name.
Command Mode	Global configuration mode
Usage Guide	**eportalv2** indicates the default template of Ruijie Second-Generation Web Authentication.

Configuring the IP Address of the Portal Server

Command	**ip** { *ip-address* | *ipv6-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the Webauth URL of the Portal Server

Command	**url** { *url-string* }
Parameter Description	Indicates the Webauth URL of the portal server.
Command Mode	Webauth template configuration mode

Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Webauth URL

Command	**fmt { cmcc-ext1 | cmcc-normal | ruijie }**
Parameter Description	Indicates the format of the Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	**fmt** must be set to **cmcc-ext1**.

Configuring the Webauth Communication Key

- (Mandatory) To enable Ruijie Second-Generation Web Authentication, you must configure the key used for the communication between the NAS or convergence device and portal server.
- When the NAS finds an unauthenticated client attempting to access network resources, it redirects the client to the specified Webauth URL, where the client can initiate authentication to the portal server. During the authentication process, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Command	**web-auth portal key** { *key-string* }
Parameter Description	*key-string*: Indicates the Webauth communication key used for the communication between the NAS and portal server. The key contains up to 255 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Detection Interval and Traffic Threshold for MAC Address-based SMS Authentication

- After an STA is associated with the WLAN enabled with MAC address-based SMS authentication, a free data quota is allocated to the STA. When the STA uses up the traffic allowed during the specified time period, a MAC address binding status query is triggered.

Command	**web-auth sms-flow interval** *interval* **threshold** *flows*
Parameter Description	*interval*: Indicates the detection interval, in the unit of minutes. *flows*: Indicates the flow threshold, in the unit of KB.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Portal Server Bound for MAC Address-based SMS Authentication

- Mandatory.

Command	**web-auth bind-portal** *string* **[type {** *local-spec* **|** *group-spec***}]**
Parameter	*string*: Indicates a Webauth template.

Description	
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Setting the winterface Field in the Redirection URL

- China Mobile's MAC address-based specification requires that the redirection URL carry the **winterface** field, which must be configurable based on a WLAN.

Command	**web-auth winterface** *string*
Parameter Description	*string*: Indicates **winterface** field.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Setting the AC IP Field in the Redirection URL

- China Mobile's MAC address-based specification requires that the redirection URL carry the **AC IP** field. Because an AC may have multiple IP addresses, a configuration command is provided to configure an IPv4 address on the specified WLAN, and the IPv4 address specifies the value of the **AC IP** field in the redirection URL.

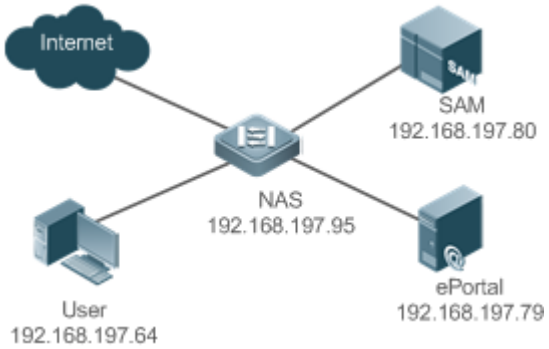
Command	**web-auth wlan-ac-ip** *ipv4*
Parameter Description	*ipv4:* Indicates the **AC IP** field.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

- Check that unauthenticated clients can access the Internet before the traffic threshold is reached.
- Check that authentication is triggered when the traffic threshold is reached.

Configuration Example

Configuring MAC Address-Based SMS Authentication

Scenario **Figure 1-10**	
Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS-server host and communication key on the NAS. ● Configure the default AAA method lists for Web authentication and accounting on the NAS. ● Configure the IP address of the portal server and the Webauth communication key (ruijie) used for communicating with the portal server on the NAS. ● Configure the Webauth URL on the NAS. ● Configure the detection interval and traffic threshold for MAC address-based SMS authentication, and set the **winterface** and **AC IP** fields on the NAS. ● Enable MAC address-based SMS authentication for WLANSEC1 on the NAS.
	`Ruijie#configure` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#aaa new-model`
	`Ruijie(config)#radius-server host 192.168.197.79 key ruijie`
	`Ruijie(config)#aaa authentication web-auth default group radius` `Ruijie(config)#aaa accounting network default start-stop group radius`
	`Ruijie(config)#web-auth template eportalv2` `Ruijie(config.tmplt.eportalv2)#ip 192.168.197.79` `Ruijie(config.tmplt.eportalv2)#exit` `Ruijie(config)#web-auth portal key ruijie`
	`Ruijie(config)# web-auth template eportalv2` `Ruijie(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp` `Ruijie(config.tmplt.eportalv2)#fmt cmcc-ext1` `Ruijie(config.tmplt.eportalv2)#exit`
	`Ruijie(config)# web-auth sms-flow interval 5 threshold 10`

	Ruijie(config)# wlansec 1 Ruijie(config-wlansec)# web-auth bind-portal eportalv2 Ruijie(config-if-range)# exit
Verification	● Check whether Web authentication is configured successfully.
	Ruijie(config)#show running-config … aaa new-model aaa authentication web-auth default group radius aaa accounting network default start-stop group radius … radius-server host 192.168.197.79 key ruijie … web-auth template eportalv2 ip 192.168.197.79 url http://192.168.197.79:8080/eportal/index.jsp fmt cmcc-ext1 ! web-auth portal key ruijie web-auth sms-flow interval 5 threshold 10 … wlansec 1 web-auth bind-portal eportalv2 ! interface GigabitEthernet 0/3 web-auth enable eportalv2

Common Errors

- The communication key between the portal server and NAS is configured incorrectly or only on the portal server or NAS, causing authentication errors.
- The communication parameters of the RADIUS server and NAS are set incorrectly, causing authentication errors.
- The portal server does not support the CMCC WLAN Service Portal Specification, causing compatibility failure.

1.4.6. Configuring WeChat Web Authentication

Configuration Effect

- Redirect unauthenticated mobile phone users with WLAN association to a WeChat-based one-click Wi-Fi connection page displayed on the mobile phone browser. A user can tap a link on the page to wake up the WeChat client and use it to perform Wi-Fi connection authentication.
- Allow unauthenticated mobile phone users to scan a QR code to perform Wi-Fi connection authentication through WeChat.
- Redirect unauthenticated PC users with WLAN association to a WeChat-based one-click Wi-Fi connection page displayed on the PC browser. A user can scan a QR code on the page by using the mobile phone associated with the same WLAN as the PC to enable the PC to perform authentication to access the Internet.

Notes

- WeChat Web authentication is supported only on wireless devices.

Configuration Steps

Creating a Wechat Webauth Template

- (Mandatory) To enable WeChat Web authentication, you must create a template.

Command	**web-auth template** {**wechat	(***portal-name* **wechat**)}
Parameter Description	Indicates the name of the customized template for WeChat Web authentication
Command Mode	Global configuration mode
Usage Guide	**wechat** is the name of the default template of WeChat-based Wi-Fi connection authentication.

Configuring the IP Address of the Portal Server

- (Mandatory) To enable WeChat Web authentication, you must configure the IP address of the portal server.

Command	**ip***ip-address*
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuring the WeChat Webauth URL

- (Mandatory) To enable WeChat Web authentication, you must configure the WeChat Webauth URL address of the portal server.

Command	**service-url** { *url-string* }

Parameter Description	Indicates the WeChat Webauth URL.
Command Mode	Webauth template configuration mode
Usage Guide	Configure only the domain name, which must not start with **http://** or **https://**.

Configuring the Authentication Page Address for the Portal Server

- The function is optional for devices of version 11.1(5)B9 and the default configuration can be used.

Command	**url** { *url-string* }
Parameter Description	**url**: Indicates the URL address of the server.
Command Mode	Template configuration mode of web authentication
Usage Guide	The authentication page address starts with **http://** or **https://**.

Configuring the Webauth Communication Key

- (Mandatory) To enable WeChat Web authentication, you must configure the communication key of the portal server.

Command	**key** *key-string*
Parameter Description	*key-string*: Indicates the communication key of the portal server. You need to configure a key used for the communication between the NAS and authentication server. The key contains up to 255 characters.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the communication keys configured on the portal server and the NAS are the same; otherwise, interworking will fail.

Configuring the NAS ID

- It is optional in standalone-node scenarios but mandatory in hot backup and VAC scenarios.

Command	**nas-id** *nas-id-string*
Parameter Description	*nas-id-string*: Sets this parameter to the serial number of the device by default.
Command Mode	AC configuration mode
Usage Guide	Configure the NAS ID in hot backup and VAC scenarios to ensure that all ACs have only one serial number.

Enabling the Smart WeChat Web Authentication

- Optional.

Command	**web-auth sta-perception enable**
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	Enable the smart authentication based on customer's requirements. Run the **ip dhcp snooping** command before the smart authentication takes effect.

Enabling the Single Escape Function

- With the escape function, if the number of authorization requests that an STA sends exceeds the configured value, but no successful authentication is achieved, then the NAS lets the STA escape and permits the corresponding entry to pass.

Command	**escape user-try-auth** *counts* **online-time** *minutes*
Parameter Description	*counts*: Indicates the number of authorization requests an STA sends. It's recommended to set this value to 4. *minutes:* Indicates how long an escaping STA can access the Internet.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling the Escape Function

- After configuration, if the server is unreachable or the server allows STAs to escape, later access STAs are exempted from authentication and permitted to escape. The escape duration is specified by the **interval** *minutes* parameter.
- Configuration in WLAN security configuration mode takes priority over that in global configuration mode. If this command is run in global configuration mode but not in WLAN security configuration mode, then the configuration in global configuration takes effect.
- To cancel escape, run the **web-auth wechat-escape recover** command in global configuration mode.

Command	**web-auth wechat-escape interval** *minutes*
Parameter Description	*minutes*: Indicates the maximum online time for escape users in the unit of minutes. The default value is 60min.
Command Mode	Global configuration mode, WLAN security configuration mode
Usage Guide	N/A

Configuring Server Detection

- (Optional) After the function is configured, the device detects the server. If it fails to receive the server response or the response is unavailable within a certain interval and the collective escape function is configured on the device, all users who gain access later are permitted to pass without authentication.
- To cancel server detection, run the **no web-auth wechat-check** command in global configuration mode.

Command	**web-auth wechat-check interval** *minutest*
Parameter	*minutes*: Indicates the timer interval for server detection. The unit is minutes and there is no default value.

Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Smart IP Address Check

- (Optional) After smart IP address check is configured, the STAs that fail to obtain IP addresses after the specified time has elapsed are forced offline.

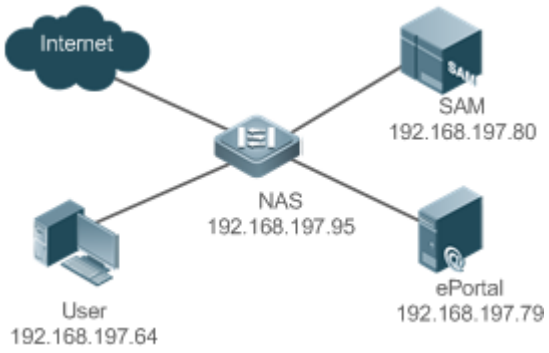
Command	**web-auth valid-ip-acct[timeout** *seconds***]**
Parameter Description	*seconds*: Indicates the time during which STAs can attempt to obtain IP addresses in the unit of seconds. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check whether unauthenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Configuration Example

Configuring WeChat Web Authentication

Scenario Figure 1-11	
Configuration Steps	● Configure the IP address 192.168.58.110 of the domain name server on the NAS. ● Configure the WeChat Webauth template on the NAS. ● Configure the IP address and Webauth URL on the NAS. ● Configure the communication key (ruijie) used for communicating with the portal server on the NAS. ● Configure the IP address used for external communication on the NAS. ● Apply the template to WLANSEC1 and enable WeChat Web authentication.
	`Ruijie#configure` `Enter configuration commands, one per line.  End with CNTL/Z.`

	Ruijie(config)#ip name-server 192.168.58.110
	Ruijie(config)#web-auth template wechat
	Ruijie(config.tmplt.wechat)#ip 192.168.197.79 Ruijie(config.tmplt.wechat)#service-url wmc.ruijie.com.cn
	Ruijie(config.tmplt.wechat)#key ruijie
	Ruijie(config.tmplt.wechat)#nas-ip 1.1.1.1
	Ruijie(config.tmplt.wechat)#exit
	Ruijie(config)# wlansec 1 Ruijie(config-wlansec)# web-auth portal wechat Ruijie(config-wlansec)# webauth
Verification	Check whether Web authentication is configured successfully.
	Ruijie(config)#show running-config … ip name-server 192.168.58.110 … web-auth template wechat ip 192.168.197.79 service-url wmc.ruijie.com.cn http://192.168.197.79:8080/eportal/index.jsphttp://192.168.197.79:8080/eportal/index.jsp key ruijie nas-ip 1.1.1.1 !… wlansec 1 web-auth portal wechat webauth !

Common Errors

- The key used for the communication between the portal server and NAS is configured incorrectly, or encryption is configured only on the portal server or NAS, causing abnormal authentication.
- The IP address of the NAS is configured as a straight-through address, and authentication packets cannot be received, causing an authentication failure.
- The IP address of the domain name server is not configured, causing a whitelist resolution failure. The IP address of the WeChat server is not permitted to pass.
- The ip dhcp snooping, ip dhcp snooping trust, and web-auth sta-perception enable commands are not executed when smart authentication is enabled, causing a failure of the smart authentication during second-time authentication.

1.4.7. Specifying an Authentication Method List

Configuration Effect

- The portal server sends an authentication request to the NAS when a user submits authentication information. The NAS resolves the authentication server information and other information based on the configured authentication method list name before initiating authentication.
- The NAS selects the authentication server based on the specified authentication method list.

Notes

- Before you configure an authentication method list name, ensure that the authentication methods in the list have been configured on the AAA module. The command used to configure authentication methods on the AAA module is **aaa authentication web-auth** { *default* | *list-name* }*method1 [method2*...].
- Different authentication methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default authentication method is used if no authentication method list is configured. Run the **authentication** { *mlist-name* } command to configure an authentication method list name when the authentication method list name on the AAA module needs to be modified or multiple method lists exist.

Verification

- Configure two authentication method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Create user a and configured a password for the user on server 1. Create user b on server 2.
- Configure the use of list 1.
- Perform authentication as user b and check that authentication fails.
- Perform authentication as user a and check that authentication is successful.

Related Commands

↘ **Specifying an Authentication Method List**

Command	**authentication** {*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured authentication method list name is consistent with that on the AAA module.

Configuration Example

Specifying an Authentication Method List

Configuration Steps	● Specify the authentication method list **mlist1**.
	`Ruijie(config.tmplt.iportal)#authentication mlist1`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: eportalv2` `Url: http://17.17.1.21:8080/eportal/index.jsp` `Ip: 17.17.1.21` `BindMode: ip-only-mode` `Type: v2` `Port: 50100` `State: Active` `Acctmlist: default` `Authmlist: mlist1`

1.4.8. Specifying an Accounting Method List

Configuration Effect

- The NAS sends an accounting request when a user passes authentication. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.
- Specify an accounting method list for the NAS to perform accounting.

Notes

- Ensure that the accounting method list has been configured on the AAA module. The command used to configure accounting methods on the AAA module is **aaa accounting network** {**default** | *list-name* }start-stop method1 [method2...].
- Different accounting methods for IPv4 authentication and IPv6 authentication are not supported.

Configuration Steps

- Optional.
- The default accounting method is used if no accounting method list is configured. Run the **accounting** {*mlist-name* } command to configure an accounting method list name when the accounting method list name on the AAA module needs to be modified or multiple method list names exist.

Verification

- Configure two accounting method lists on the AAA module. Apply list 1 to server 1 and list 2 to server 2.
- Configure the use of list 1.
- Use a valid account to perform authentication to access the Internet.
- View user accounting information on server1 and server2. Check that the user accounting information exists only on server1.

Related Commands

Specifying an Accounting Method List

Command	**accounting**{*mlist-name*}
Parameter Description	Indicates a method list name.
Command Mode	Webauth template configuration mode
Usage Guide	Ensure that the configured accounting method list name is consistent with that on the AAA module.

Configuration Example

Specifying an Accounting Method List

Configuration Steps	● Specify the accounting method list **mlist1**.
	`Ruijie(config.tmplt.eportalv2)#accounting mlist1`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:`

Configuration Steps	● Specify the accounting method list **mlist1**.
	`Ruijie(config.tmplt.eportalv2)#accounting mlist1`
Verification	● Check whether the configuration is successful.
	`------------------------------------------------------------` `Name: eportalv2` `Url: http://17.17.1.21:8080/eportal/index.jsp` `Ip: 17.17.1.21` `BindMode: ip-mac-mode` `Type: v2` `Port: 50100` `State: Active` `Acctmlist: mlist1` `Authmlist: mlist1`

1.4.9. Configuring the Communication Port of the Portal Server

Configuration Effect

- When the NAS detects that a user logs out, it notifies the portal server. The NAS interacts with the portal server through the portal specification, which specifies the port number used to listen to and send/receive packets.
- When the listening port of the portal server is changed, the communication port of the portal server must be modified on the NAS to enable the NAS to interact with the portal server.
- In Ruijie iPortal Web Authentication, this function is used to configure the HTTP listening port of the NAS. The default port number is 8081.

Notes

- The configured port number must be consistent with the port actually used by the portal server.
- This function is applicable to Ruijie Second-Generation Web Authentication and iPortal Web Authentication. The two authentication schemes use different default port numbers. In Ruijie Second-Generation Web Authentication, the configured port number is used for the interaction between the NAS and portal server through the portal specification. In Ruijie iPortal Web Authentication, the configured port number is used for packet listening on the NAS.

Configuration Steps

- Optional.

- Run the **port** *port-num* command to maintain port configuration consistency when the portal server does not use the default port number or the listening port of the NAS conflicts with other port and needs to be adjusted.

Verification

- Configure Ruijie Second-Generation Web Authentication.
- Change the listening port of the server to 10000.
- Run the **port** *port-num* command to configure the port number 10000.
- Simulate the scenario where a user performs authentication to access the Internet.
- Force the user offline on the NAS, refresh the online page, and check that a user logout notification is displayed.

Related Commands

Configuring the Communication Port of the Portal Server

Command	**port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Communication Port of the Portal Server

Configuration Steps	● Configure the communication port of the portal server as port 10000.
	`Ruijie(config.tmplt.eportalv2)#port 10000`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: eportalv2` `Url: http://17.17.1.21:8080/eportal/index.jsp` `Ip: 17.17.1.21` `BindMode: ip-only-mode` `Type: v2` `Port: 10000`

Configuration Steps	● Configure the communication port of the portal server as port 10000.
	`Ruijie(config.tmplt.eportalv2)#port 10000`
Verification	● Check whether the configuration is successful.
	`Acctmlist:` `Authmlist:`

1.4.10. Specifying the Webauth Binding Mode

Configuration Effect

- When a user goes online, the user's entry needs to be written to a forwarding rule. The forwarding rule mapping method can be modified by specifying different binding modes, which further affects the Internet access rules applied to users. In IP-only mode, all the packets carrying the specified IP address are permitted to pass, and the STAs who send the packets can access the Internet. In IP+MAC mode, only the packets carrying both the specified IP address and MAC address are permitted to pass, and the STAs who send the packets can access the Internet.

Notes

- In Layer-3 authentication, the MAC addresses visible to the NAS are the gateway addresses of STAs. Because these MAC addresses are not accurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default Webauth binding mode is IP+MAC.
- Determine a binding mode based on the accuracy of user information obtained by the NAS. When the IP and MAC addresses of STAs are accurate (in L2 authentication, for example), IP+MAC is recommended. When the IP and MAC addresses are not accurate, select IP-only.

Verification

- Change the binding mode to IP-only.
- Simulate the scenario where a user performs authentication to access the Internet.
- Modify the MAC address of the user, or use a client with the same IP address but a different MAC address to access the Internet.
- Check that the user accesses the Internet normally.

Related Commands

↘ Specifying the Webauth Binding Mode

Command	**bindmode {ip-mac-mode | ip-only-mode}**
Parameter	**ip-mac-mode**: Indicates IP-MAC binding mode.

Description	**ip-only-mode**: Indicates IP-only binding mode.
Command Mode	Webauth template configuration mode
Usage Guide	N/A

Configuration Example

Specifying the Webauth Binding Mode

Configuration Steps	● Set the binding mode to IP-only.
	`Ruijie(config.tmplt.eportalv2)#bindmode ip-only-mode`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: eportalv2` `Url: http://17.17.1.21:8080/eportal/index.jsp` `Ip: 17.17.1.21` `BindMode: ip-only-mode` `Type: v2` `Port: 10000` `Acctmlist:` `Authmlist:`

1.4.11. Customizing a Page Suite

Configuration Effect

- Configure a page suite to be used on the iPortal server and add special content or information to the page suite, for example, a logo or notice.

Notes

- A page suite must be downloaded manually to the flash memory of the NAS and saved to the ./portal directory. If the page suite is not saved or is saved to an incorrect directory, page push will fail, causing Web authentication invalid. The default page suite can be used if there are no special requirements.
- For details, see section 1.4.36 "Customizing a Page Suite."

Configuration Steps

- (Optional) By default, the default page suite is used.

Verification

- Configure Ruijie iPortal Web Authentication.
- Download a page suite.
- Specify the page suite.
- Check whether the page suite is applied to the login page.

Related Commands

Customizing a Page Suite

Command	**page-suit** *filename*
Parameter Description	*filename*: Indicates the file name of a page suite.
Command Mode	Webauth template configuration mode
Usage Guide	Download the page suite to be used to the **./porta/zipl** directory of the flash memory in advance.

Configuration Example

Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	`Ruijie(config.tmplt.iportal)#page-suitruijiepage`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: iportal` `Page-suit: ruijiepage` `Advertising url: default` `Advertising mode: online-popup` `Type: Intral Portal` `Acctmlist:default`

Configuration Steps	● Customize a page suite.
	`Ruijie(config.tmplt.iportal)#page-suitruijiepage`
Verification	● Check whether the configuration is successful.
	`Authmlist:default`

1.4.12. Configuring the Advertisement Pushing Mode

Configuration Effect

- Optional. Advertisements are pushed before or after authentication.

Notes

- By default, advertisements are pushed after authentication is successful.
- To ensure that only advertisements are pushed in the case that users are not authenticated, select the advertising function. For details, see the advertising configuration manual.

Configuration Steps

- (Optional) By default, advertisements are pushed after the authentication is successful.

Verification

- Configure embedded portal Web authentication.
- Configure a URL address that can access the Internet.
- When a user accesses the network, check whether a new window is displayed after the authentication is successful and whether information on a page of a specific URI is displayed.

Related Commands

↘ Configuring the Advertisement Pushing Address

Command	**login-popup** *url*
Parameter Description	*url*: Indicates the address pushed before authentication (during login).
Command Mode	Webauth template configuration mode
Usage Guide	
Command	**online-popup** *url*
Parameter Description	*url*: Indicates the address pushed after the authentication is successful.
Command	Webauth template configuration mode

Mode	
Usage Guide	

Configuration Example

Configuring the Advertisement Pushing Mode

Configuration Steps	● Configure the advertisement pushing mode to advertisement pushing before authentication.
	`Ruijie(config.tmplt.iportal)#login-popup http://www.ruijie.com.cn/`
Verification	● Check whether the advertisement pushing mode is configured successfully.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: iportal` `BindMode: ip-mac-mode` `Type: intra` `Port: 8081` `time_interval: 1` `Login_popup: http://www.ruijie.com.cn/` `Online_popup: (null)` `Suitename: default` `Authentication:` `Accounting:`

1.4.13. Configuring the Format of the Webauth URL

Configuration Effect

- Configure the URL used for redirecting users to the portal server based on the customized parameters.

Notes

- The parameter sequence of the customized URL may not be consistent with the parameter sequence of the actual URL.

Configuration Steps

- Optional.

Verification

- Configure a customized URL.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected and the parameters of the redirection URL are consistent with those of the customized URL.

Related Commands

Configuring the Format of the Webauth URL

Command	**fmt custom [encryp { md5 | des | des_ecb | des_ecb3 | none }] [user-ip** *userip-str***] [user-mac** *usermac-str***mac-format [dot | line | none]][user-vid** *uservid-str***]** [**user-id** *userid-str*] **[nas-ip** *nasip-str* **][nas-id** *nasid-str***][nas-id2** *nasid2-str***] [ac-name** *acname-str***][ap-mac** *apmac-str* **mac-format [dot | line | none]][url** *url-str***] [ssid** *ssid-str* **][port** *port-str* **][ac-serialno** *ac-sno-str* **][ap-serialno** *ap-sno-str***] [additional** *extern-str***]**
Parameter Description	*userip-str*: Indicates the parameter name mapped to the IP address of an STA. *usermac-str*: Indicates the parameter name mapped to the MAC address of an STA. *uservid-str*: Indicates the parameter name mapped to the VID of an STA. *userid-str*: Indicates the parameter name mapped to the ID of an STA. *nasip-str*: Indicates the parameter name mapped to the IP address of the NAS. *nasid-str*: Indicates the parameter name mapped to the ID of the NAS. *nasid2-str*: Indicates the parameter name mapped to the ID of the NAS. (Two NAS IDs can be configured.) *ac-name*: Indicates the parameter name mapped to the name of the NAS. *apmac-str*: Indicates the parameter name mapped to the MAC address of the associated AP. *url-str*: Indicates the parameter name mapped to the original URL that the STA accesses. *ssid-str*: Indicates the parameter name mapped to the SSID. *port-str*: Indicates the parameter name mapped to the user authentication port. *ac-sno-str*: Indicates the parameter name mapped to the serial number of the AC. *ap-sno-str*: Indicates the parameter name mapped to the serial number of the NAS. *extern-str*: Indicates a fixed character string. Some portal servers must be identified by character strings. *md5*: Indicates MD5 mode. *des*: Indicates DES mode. *des_ecb*: Indicates DES_ECB mode. *des_ecb3*: Indicates DES_ECB3 mode. *none*: Indicates no encryption.
Command Mode	Template configuration mode
Usage Guide	You can add or delete individual parameters.

Configuration Example

Configuring the Format of the Webauth URL

Configuration Steps	● Configure the plaintext IP address and MAC address of an STA,IP address of the NAS, SSID, URL, and other parameters as the redirection URL parameters.
	`Ruijie(config.tmplt.eportalv2)# fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firstu`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl`

1.4.14. Configuring the Redirection HTTP Port

Configuration Effect

- When an STA accesses network resources (for example, the user accesses the Internet using a browser), the STA sends HTTP packets. The NAS or convergence device intercepts these HTTP packets to determine whether the STA is accessing network resources. If the NAS or convergence device detects that the STA is not authenticated, it prevents the STA from accessing network resources and displays an authentication page to the STA. By default, the NAS intercepts the HTTP packets that STAs send to port 80 to determine whether STAs are accessing network resources.
- After a redirection HTTP port is configured, the HTTP requests that STAs send to the specified destination port can be redirected.

Notes

- The commonly used management ports on the NAS or convergence device, such as ports 22, 23 and 53, and ports reserved by the system are not allowed to be configured as the redirection port. All ports except port 80 with numbers smaller than 1000 are seldom used by the HTTP protocol. To avoid a conflict with the well-known TCP port, do not configure a port with a small number as the redirection port unless necessary.

Configuration Steps

- Optional.
- When you configure automatic client acquisition, if you need to enable the NAS to intercept the HTTP packets that STAs send to the specified destination port, configure a redirection HTTP port.

Verification

- Configure an interception port.
- Open the browser of a PC and access the Internet through the port without performing authentication.
- Check whether the access requests are redirected to an authentication page.

Related Commands

Configuring the Redirection HTTP Port

Command	**http redirect port** *port-num*
Parameter Description	*port-num*: Indicates the port number.
Command Mode	Global configuration mode
Usage Guide	A maximum of 10 different destination port numbers can be configured, not including default ports 80 and 443.

Configuration Example

Configuring the Redirection HTTP Port

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	`Ruijie(config)#http redirect port 8080`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show web-auth rdport` `Rd-Port:` `80 443 8080`

1.4.15. Configuring Rate Limit Webauth Logging

Configuration Effect

- The Web authentication module sends syslog messages to the administrator to display the information and relevant events of users who perform login/logout. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at a certain rate.

Notes

- When the login/logout rate is high, syslog messages are output frequently, which affects device performance and results in spamming.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login/logout.

Verification

- Configure logging rate limiting.
- Check whether users log in and out at a certain rate.
- Check that syslog messages are printed out at the limit rate.

Related Commands

Configuring Rate Limit Webauth Logging

Command	**web-auth logging enable** *num*
Parameter Description	*num*: Indicates the syslog output rate (entry/second).
Command Mode	Global configuration mode
Usage Guide	When the syslog output rate is set to **0**, syslog messages are output without limit. The output of syslog messages of the critical level and syslog messages indicating errors is not limited.

Configuration Example

Configuring Rate Limit Webauth Logging

Configuration Steps	● Disable rate limit Webauth Logging.
	`Ruijie(config)#web-auth logging enable 0`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth logging enable 0` `...`

1.4.16. Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Effect

- When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The NAS or convergence device intercepts the HTTP packets and redirects the user to a Web authentication page. To prevent an unauthenticated user from initiating too many HTTP connection requests and save resources on the NAS, it is necessary to limit the maximum number of HTTP sessions that the unauthenticated user can initiate on the NAS.
- A user occupies an HTTP session when performing authentication, and the other application programs of the user may also occupy HTTP sessions. For this reason, it is recommended that the maximum number of HTTP sessions for an

unauthenticated user be not set to 1. By default, each unauthenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by unauthenticated clients.

Notes

- If the authentication page fails to be displayed during Web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that may occupy HTTP sessions and then perform Web authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each unauthenticated user can initiate and the maximum number of HTTP sessions that unauthenticated clients can initiate on each port.
- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Modify the maximum number of HTTP sessions that an unauthenticated user can initiate.
- Simulate the scenario where an unauthenticated user constructs identical sessions to connect to the NAS continuously.
- Simulate the scenario where the unauthenticated user accesses the Internet using a browser. Check whether the access requests are redirected and the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

↘ Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Command	**http redirect session-limit** { *session-num* }[**port** { *port-session-num* }]
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for unauthenticated clients. The value range is 1 to 255. The default value is 255. *port-session-num*: Indicates the maximum number of HTTP sessions on each port for authenticated clients. The value range is 1 to 65,535. The default value is 300.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Maximum Number of HTTP Sessions for Unauthenticated Clients

Configuration Steps	● Set the maximum number of HTTP sessions for unauthenticated clients to 3.
	`Ruijie(config)#http redirect session-limit 3`

Verification	• Check whether the configuration is successful.
	Ruijie(config)#show web-auth parameter HTTP redirection setting: session-limit: 3 timeout: 3 Ruijie(config)#

1.4.17. Configuring the HTTP Redirection Timeout

Configuration Effect

- Configure the HTTP redirection timeout to maintain redirection connections. When an unauthenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted and re-established with the NAS or convergence device. Then, the NAS or convergence device waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection timeout is intended to prevent the user from occupying the TCP connection for a long time without sending GET/HEAD packets. By default, the timeout for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout for maintaining redirection connections.

Verification

- Change the timeout period.
- Use a network packet delivery tool to set up a TCP connection.
- View the status of the TCP connection on the NAS. Check whether the TCP connection is closed when the timeout is reached.

Related Commands

↘ Configuring the HTTP Redirection Timeout

Command	**http redirect timeout** { *seconds* }
Parameter Description	*Seconds*: Indicates the timeout for maintaining redirection connections, in the unit of seconds. The value ranges from 1 to 10. The default value is 3s.
Command Mode	Global configuration mode

Usage Guide	N/A

Configuration Example

Configuring the HTTP Redirection Timeout

Configuration Steps	● Set the HTTP redirection timeout to 5s.
	`Ruijie(config)#http redirect timeout 5`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show web-auth parameter` `HTTP redirection setting:` `  session-limit: 255` `  timeout:       5`

1.4.18. Configuring the Straight-Through Network Resources

Configuration Effect

- After Web authentication or 802.1Xauthentication is enabled on a port, the users connecting to the port need to pass Web authentication or 802.1Xauthentication before accessing network resources.
- Perform this configuration to exempt users from authentication when accessing some network resources.
- If a website is configured as a network resource of authentication exemption, all users, including unauthenticated clients, can access the website. By default, authentication exemption is not configured, and unauthenticated clients are not allowed to access network resources.
- IPv6 is supported.

Notes

- The maximum number of free resources and the maximum number of unauthenticated clients cannot exceed 1000 respectively. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be set.
- **http redirect direct-site** is used to configure the straight-through URL address for users, and **http redirect** is used to configure the straight-through IP address of the Web authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. It is recommended not to configure the IP address of the Web authentication server by using **http redirect direct-site**.
- When IPv6 addresses are used, you need to allow local link address learning. If this function is not configured, the NAS cannot learn the MAC addresses of clients.

Configuration Steps

- Optional.
- Run the **http redirect direct-site** command to enable unauthenticated clients to access network resources.

Verification

- Configure the straight-through network resources.
- Check whether unauthenticated clients can access the configured network resources using PCs.

Related Commands

Configuring the Straight-Through Network Resources

Command	**http redirect direct-site** { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**]}
Parameter Description	*ipv6-address*: Indicates the IPv6 address of the network exempt from authentication. *ipv4-address*: Indicates the IPv4 address of the network exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the network exempt from authentication.
Command Mode	Global configuration mode
Usage Guide	To set authentication-exempted ARP resource, use the **http redirect direct-arp** command preferentially.

Configuration Example

Configuring the Straight-Through Network Resources

Configuration Steps	● Configure the straight-through network resources as 192.168.0.0/16.
	`Ruijie(config)#http redirect direct-site 192.168.0.0 255.255.0.0`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show web-auth direct-site` `Direct sites:` `  Address  Mask  ARP Binding Group` `  ---------- ---------- ---------- ----------` `  192.168.0.0  255.255.0.0  Off  N/A` `Ruijie(config)#`

1.4.19. Configuring the Straight-Through ARP Resource Range

Configuration Effect

When ARP check or similar functions are enabled, the ARP learning performed by clients is controlled. As a result, clients cannot learn the ARPs of the gateway and other devices, which affects user experience. You can configure the straight-through ARP resource range to permit the ARP learning packets destined for the specified address to pass.

Notes

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the Layer-2 access device as a straight-through ARP resource. Note the following point when you perform the configuration:
- When you configure straight-through websites and ARP resources in the same address or network segment, the **http redirect direct-arp** command automatically combines the websites and ARP resources. If no ARP option is specified for the configured websites, an ARP option will be automatically added after the combination.
- When ARP check is enabled, if the outbound addresses of the PCs connecting to the Layer-2 access device are not the gateway address, configure the outbound addresses as straight-through ARP resources. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.

Configuration Steps

- Optional.
- If ARP check is enabled on the NAS, you must configure the free resources and gateway address as straight-through ARP resources.

Verification

- Configure straight-through ARP resources.
- Clear the ARP cache of the PC of an unauthenticated user. (Run the **arp -d** command in the Windows operating system.)
- Run the **ping** command on the PC to access the straight-through ARP resources.
- View the ARP cache on the PC (run the **arp -a** command in the Windows operating system) and check whether the PC learns the ARP address of the straight-through ARP resources.

Related Commands

Configuring the Straight-Through ARP Resource Range

Command	**http redirect direct-arp** {*ip-address* [*ip-mask*] }
Parameter Description	*ip-address*: Indicates the IP address of free resources. *ip-mask*: Indicates the mask of free resources.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Straight-Through ARP Resource

Configuration Steps	● Configure the straight-through ARP resource as 192.168.0.0/16.
	`Ruijie(config)#http redirect direct-arp 192.168.0.0 255.255.0.0`

Verification	● Check whether the configuration is successful.
	Ruijie(config)#show web-auth direct-arp Direct arps: Address Mask --- --- 192.168.0.0 255.255.0.0 Ruijie(config)#

1.4.20. Configuring an Authentication-Exempted Address Range

Configuration Effect

- Exempt users from Web authentication when accessing reachable network resources. By default, no authentication-exempted address range is configured. All users must pass Web authentication before accessing network resources.
- The authentication-exempted address range can be configured as an IP address range or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure an authentication-exempted user.
- Check whether the user can access the Internet without authentication.

Related Commands

↘ Configuring an Authentication-Exempted Address Range

Command	**web-auth direct-host** { *ipv4-address* [*ip-mask*] [**arp**] | *ipv6-address* | *mac-address*][**port** *interface-name*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the user exempt from authentication. *ipv6-address*: Indicates the IPv6 address of the user exempt from authentication. *ip-mask*: Indicates the mask of the IPv4 address of the user exempt from authentication. *interface-name*: Indicates the name of the interface on which authentication exemption is enabled.

	mac-address: Indicates the MAC address of the user exempt from authentication.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used to assign pass permissions to ARP packets. This field must be set when ARP check is enabled. After the **port** field is set, authentication exemption takes effect only on the configured interface.

Configuration Example

Configuring an Authentication-Exempted Address Range

Configuration Steps	● Configure an authentication-exempted address range.
	`Ruijie (config)# web-auth direct-host 192.168.197.64`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show web-auth direct-host` `Direct hosts:` `Address Mask Port ARP Binding Group` `192.168.197.64 255.255.255.255 Off N/A` `Ruijie(config)#`

1.4.21. Configuring the Interval for Updating Online User Information

Configuration Effect

- The NAS or convergence device maintains and periodically updates the information of online users, including users' online duration, to monitor the usage of network resources. When the online duration threshold is reached, users will be prevented from using network resources.

Notes

- The user information updating interval must be configured as 60 or multiple of 60; otherwise, the system will select the minimum multiple of 60 above and closest to the actual configuration as the interval.

Configuration Steps

- Optional.
- Perform this configuration to allow unauthenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View the information of online users after the update interval has elapsed.

Related Commands

Configuring the Interval for Updating Online User Information

Command	**web-auth update-interval** *{ seconds }*
Parameter Description	*seconds*: Indicates the interval for updating online user information, in the unit of seconds. The value ranges from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default updating interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

Configuring the Interval for Updating Online User Information

Configuration Steps	● Set the interval for updating online user information to 60s.
	`Ruijie (config)# web-auth update-interval 60`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show run | include web-auth update-interval` `web-auth update-interval 60`

1.4.22. Configuring Portal Detection

Configuration Effect

- Detect the availability of the active portal server periodically. When the active portal server is unavailable, the standby portal server takes over the services.
- Ruijie Second-Generation Web Authentication provides two detection methods. One is that the NAS constructs and sends portal packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Another is the NAS sends ping packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available. Because some servers or intermediate network segments filter ping packets, the first method is commonly used. The ping detection method is only used based on special requirements. In Ruijie First-Generation Web Authentication, the NAS connects to a port of the portal server and checks whether the port is reachable. If the portal is reachable, the NAS determines that the portal server is available.

- For the first method in the second-generation authentication, the interval of server availability detection is specified by the **interval** parameter, and the maximum number of packets that can be sent during each time of detection is specified by the **retransmit** parameter. If the portal server does not respond, the NAS determines that the portal server is unavailable. The timeout period for each packet is specified by the **timeout** parameter. The parameter settings are also supported by Ruijie First-Generation Web Authentication.
- Portal server detection takes effect for Ruijie First- and Second-Generation Web Authentication.
- If multiple portal servers are configured, these servers are working in active/standby mode.

Notes

- Multiple portal servers must be configured to realize failover when an error is detected on one server.
- Only one of the two detection methods can be used at a time in case of collision. If both detection methods are configured, a detection algorithm conflict will occur or the detection results will be inaccurate.
- The system will automatically select a detection method based on whether Ruijie First- or Second-Generation Web Authentication is used.

Configuration Steps

- Optional.
- Configure multiple portal server templates applicable to Ruijie First- or Second-Generation Web Authentication.

Verification

- Configure two portal server templates for Ruijie First- or Second-Generation Web Authentication. Make the first template point to an unavailable server and the second template point to an available server.
- When the Console displays a log indicating that the portal server is not available, simulate the scenario where a user opens a browser to perform login authentication. Check whether the user is redirected to the second portal server.

Command	**web-auth portal-check** [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries**]**
Parameter Description	*intsec*: Indicates the detection interval. The default value is 10s. *tosec:* Indicates the packet timeout period. The default value is 5s. *intsec*: Indicates the timeout retransmission times. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.
Command	**web-auth ping** [**interval** *minutes*] [**retry** *times*]
Parameter Description	*minutes*: Indicates the detection interval. The default value is 1 minute. *times*: Indicates the timeout retransmission times. The default value is 3 (times).
Command	Global configuration mode

Mode	
Usage Guide	In many network environments, only one portal server is deployed, and portal server detection does not need to be configured. If multiple portal servers exist, it is recommended that the parameters of portal server detection be not set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

Configuration Example

Configuring Portal Detection

Configuration Steps	• Configure portal detection.
	`Ruijie(config)#web-auth portal-check interval 20 timeout 2 retransmit 2`
Verification	• Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth portal-check interval 20 timeout 2 retransmit 2` `...`

1.4.23. Configuring Portal Escape

Configuration Effect

- Allow new users to access the Internet without authentication when the portal server is not available.

Notes

- To use the portal escape function, you must configure portal detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are not available.
- The escape function is intended only for the portal server, instead of the RADIUS server.

Configuration Steps

- Optional.
- Configure portal detection.
- Configure portal escape.
- (Optional) Configure the nokick attribute.

Verification

- Configure a portal server and disable the server.
- Configure the portal detection and escape functions.
- When the NAS detects that the portal server is not available, check whether a client accesses the Internet without authentication.

Related Commands

Configuring Portal Escape

Command	**web-auth portal-escape [nokick]**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure portal escape if the continuity of some critical services on the network needs to be maintained when the portal server is faulty. You must configure portal detection when you use this function. If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is deleted, the system forces users offline.

Configuration Example

Configuring Portal Escape

Configuration Steps	● Configure portal escape.
	`Ruijie(config)#web-auth portal-escape`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth portal-escape` `...`

1.4.24. Enabling DHCP Address Check

Configuration Effect

- Allow only the clients that are allocated with IP addresses through DHCP to perform authentication.

Notes

- To use the DHCP address check function, you must configure DHCP snooping.
- DHCP address check is supported only for IPv4.
- DHCP address check is applicable only to Ruijie Second-Generation Web Authentication and iPortal Web Authentication.
- The requirement that users obtain IP addresses through DHCP must be specified during network deployment. Those users cannot also use static IP addresses; otherwise, the existing users that use static IP addresses will be affected.
- If a few users need to use static IP addresses, configure these IP addresses as straight-through addresses, and these users are exempt from authentication.
- If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable the global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled in each interface.

Configuration Steps

- Optional.
- Enable DHCP snooping.
- Enable DHCP address check.

Verification

- Enable DHCP address check.
- Configure a static IP address that is not allocated by the DHCP server on a client.
- Connect the client to the Internet and check whether the STA cannot perform authentication.

Related Commands

↘ Enabling Global DHCP Address Check

Command	**web-auth dhcp-check**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure DHCP address check to allow only the users who obtain IP addresses through DHCP to access the Internet. This function helps prevent the users who configure IP addresses without authorization from performing authentication to access the Internet.

Configuration Example

↘ Enabling DHCP Address Check

Configuration Steps	● Enable global DHCP address check.

	`Ruijie(config)#web-auth dhcp-check`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth dhcp-check` `...` `interface TenGigabitEthernet 3/1` `web-auth dhcp-check vlan 1,3-4` `...`

1.4.25. Disabling Link Detection

Configuration Effect

- The authentication entries of clients are kept when links are disconnected. The clients can access the Internet again without authentication if the IP addresses remain unchanged.
- You can disable link detection in places where mobile office is required or wireless Web authentication is deployed but wireless signal is bad.

Notes

- Do not disable link detection if clients obtain IP addresses through DHCP and the number of IP addresses in the DHCP address pool is smaller than the number of clients. If link detection is disabled, the IP address of a client that has logged out may be obtained by another client, causing a user information error.
- If link detection is disabled, a client logout action is triggered only when the user clicks the **Logout** button on the online page, the server forces the client offline, or the NAS detects low traffic on the client. It is recommended that you enable low traffic detection if you need to disable link detection. For details, see the *Configuring SCC*.
- It is recommended that you disable link detection and enable low traffic detection in a wireless environment. The reason is that the offline rate in a wireless environment is high because wireless connections are easily affected by signal interference, and disabling link detection helps improve wireless experience.

Configuration Steps

- Optional.
- Configure Web authentication.
- Disable link detection.

Verification

- Configure Ruijie-Second Generation Web Authentication and disable link detection.
- Connect a client to the Internet and perform authentication. When the client passes the authentication, disconnect from and then reconnect to the Internet with the same IP address. Check whether the client can access the Internet again without authentication.

Related Commands

Disabling Link Detection

Command	**no web-auth sta-leave detection**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can disable link detection in a wireless environment or a wired environment with the need for mobile office. To disable link detection, you must enable low traffic detection.

Configuration Example

Disabling Link Detection

Configuration Steps	● Disable link detection.
	`Ruijie(config)#no web-auth sta-leave detection`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `no web-auth sta-leave detection` `...`

1.4.26. Disabling Portal Extension

Configuration Effect

- Enable portal extension to support Ruijie portal server and portal servers that comply with the CMCC WLAN Service Portal Specification.
- You can select multiple redirection URL formats when interworking with the servers comply with the CMCC WLAN Service Portal Specification to achieve compatibility with different servers.

Notes

- Only Ruijie Second-Generation Web Authentication supports portal extension.
- Ruijie Second-Generation Web Authentication extends the CMCC WLAN Service Portal Specification. You need to determine whether to use the extension mode based on the server performance.
- If the portal server is a product of Ruijie, use the default mode, that is, extension mode. If the portal server complies with the CMCC WLAN Service Portal Specification, disable portal extension.
- The CMCC WLAN Service Portal Specification supports multiple redirection URL formats. If the portal server complies with the CMCC WLAN Service Portal Specification, select a redirection URL format supported by the server.

Configuration Steps

- Optional.
- Determine whether to disable portal extension based on the server type.
- Select a redirection URL format supported by the server if portal extension is disabled.

Verification

- Select Ruijie portal server and a portal server compliant with the CMCC WLAN Service Portal Specification to be used in Ruijie Second-Generation Web Authentication.
- Connect a client to the Internet. Check whether the client performs authentication normally on the two servers and can access the Internet.

Related Commands

Disabling Portal Extension

Command	**no web-auth portal extension**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The portal servers that comply with the *CMCC WLAN Service Portal Specification* are deployed. If Ruijie portal server is used, enable portal extension.

Configuration Example

Disabling Portal Extension

Configuration Steps	• Disable portal extension.
	`Ruijie(config)#no web-auth web-auth portal extension`
	`Ruijie(config)# http redirect url-fmt ext1`
Verification	• Check whether the configuration is successful.

Configuration Steps	● Disable portal extension.
	`Ruijie(config)#no web-auth web-auth portal extension`
	`Ruijie(config)# http redirect url-fmt ext1`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `no web-auth web-auth portal extension` `http redirect url-fmt ext1` `...`

1.4.27. Configuring a Whitelist and Blacklist

Configuration Effect

- Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.
- Blacklists and whitelists are supported based on ports, URLs, and IP addresses.

Notes

- Up to 1,000 blacklists and whitelists can be configured.
- If blacklists and whitelists are configured in the domain name format, the DNS function must be configured on the NAS so that the NAS can resolve IP addresses correctly.
- A domain name can map up to eight IP addresses.

Configuration Steps

- Optional.
- Configure DNS.
- Configure a whitelist and blacklist.

Verification

- Configure a whitelist and blacklist.
- Check whether unauthenticated STAs can access the whitelisted addresses.
- Check whether authenticated STAs cannot access the blacklisted addresses.

Related Commands

↘ **Configuring a Whitelist and Blacklist**

Command	**web-auth acl{black-ip** *ip***|black-port** *port***|black-url** *name***|white-url** *name***}**
Parameter Description	*ip*: Indicates an IP addresses blacklisted. *port*: Indicates a port numbers blacklisted. *name*: Indicates a URL blacklisted or whitelisted.
Command Mode	Global configuration mode (Blacklists can be configured in WLAN security configuration mode on wireless devices.)
Usage Guide	Configure a whitelist to allow unauthenticated clients to access some network resources, and configure a blacklist to prevent authenticated clients from accessing some network resources.

Configuration Example

↘ Configuring a Whitelist and Blacklist

Configuration Steps	● Configure a whitelist and blacklist.
	`Ruijie(config)#web-auth acl black-ip 192.168.1.2` `Ruijie(config)#web-auth acl white-url www.ruijie.com.cn`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `…` `web-auth acl black-ip 192.168.1.2` `web-auth acl white-url www.ruijie.com.cn` `…`

1.4.28. Configuring Jitter-off Accounting

Configuration Effect

- If jitter-off or low traffic detection is configured on the NAS, the time of jitter-off or low traffic detection will be accounted into the online duration. Jitter-off accounting is used to reduce the accounting error. Configure this function if the accounting policy does not allow the deduction of the anti-jitter time or low traffic detection time from the online duration.

Notes

- The NAS needs to support anti-jitter or low traffic detection.
- A client logs out for the link is disconnected for a long time or the NAS detects its low traffic.
- When the jitter-off and low traffic detection functions are enabled, the first logout is accounted with jitter-off time only. For example, the jitter-off duration is set to 5 minutes and the low traffic detection duration is set to 10 minutes; if the

client is disconnected from the network, the jitter-off function first triggers Web authentication to log the client out. In this case, only the5-minute duration is deducted from the online duration in the accounting packet.

Configuration Steps

- Optional.
- Configure the accounting function.
- Configure jitter-off or low traffic detection.
- Configure jitter-off accounting.

Verification

- Simulate the scenario where a client goes online after authentication and then offline because the low traffic threshold is reached.
- Capture the stop-accounting packet sent by the NAS and check whether the time of low traffic detection is deducted from the online duration.

Related Commands

Configuring Jitter-off Accounting

Command	**web-auth accounting jitter-off**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to include the jitter-off duration or low traffic detection time into the online duration in the stop-accounting packet based on the server accounting policy. By default, they are not included.

Configuration Example

Configuring Jitter-off Accounting

Configuration Steps	● Configure jitter-off accounting.
	`Ruijie(config)#web-auth accounting jitter-off`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth accounting jitter-off`

Configuration Steps	● Configure jitter-off accounting.
	`Ruijie(config)#web-auth accounting jitter-off`
Verification	● Check whether the configuration is successful.
	...

1.4.29. Configuring the Portal Communication Port

Configuration Effect

- Configure the port (source port) used for the communication between the NAS and portal server.

Notes

- Only one port can be configured for the communication between the NAS and portal server.

Configuration Steps

- Configure a port as the portal communication port.

Verification

- After Web authentication is enabled, capture a packet on the portal server during the authentication process and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

↘ Configuring the Portal Communication Port

Command	**ip portal source-interface** *interface-type interface-num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

↘ Configuring the Portal Communication Port

Configuration Steps	● Configure an aggregate port as the portal communication port.
	`Ruijie(config)#ip portal source-interface Aggregateport 1`

Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `ip portal source-interface Aggregateport 1`

1.4.30. Configuring a NDKEY-Compatible Webauth URL

Configuration Effect

- Configure the Webauth URL used in Web authentication to support the Shanghai NDKEY system.

Notes

- N/A

Configuration Steps

↘ Configuring a NDKEY-Compatible Webauth URL

- Set the post parameter in global configuration mode.

Command	**web-auth dkey-compatible url-parameter** *string*
Parameter Description	*string*: Indicates the value of the **post** parameter.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Execute redirection after the configuration and check that the redirection URL contains the post parameter.

Configuration Example

↘ Configuring Noise Reduction Suppression

Configuration Steps	● Configure compatibility parameters.
	`Ruijie(config)#web-auth dkey-compatible url-parameter login`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config`

Configuration Steps	● Configure compatibility parameters.
	`Ruijie(config)#web-auth dkey-compatible url-parameter login`
Verification	● Check whether the configuration is successful.
	`...` `web-auth dkey-compatible url-parameter login`

1.4.31. Enabling NAT for Ruijie iPortal Web Authentication

Configuration Effect

- Configure Ruijie iPortal Web Authentication to support NAT.

Notes

- NAT takes effect only in Ruijie iPortal Web Authentication.

Configuration Steps

↘ Enabling NAT for Ruijie iPortal Web Authentication

- Enable NAT in global configuration mode.

Command	**iportal nat enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check whether Ruijie iPortal Web Authentication can be implemented after NAT is enabled.

Configuration Example

↘ Enabling NAT for Ruijie iPortal Web Authentication

Configuration Steps	● Enable NAT for Ruijie iPortal Web Authentication.
	`Ruijie(config)#iportal nat enable`

Verification	● Check whether the configuration is successful.
	Ruijie(config)#show running-config ... iportal nat enable

1.4.32. Configuring the iPortal HTTP Retransmission Times

Configuration Effect

- Configure the iPortal HTTP retransmission times.

Notes

- The retransmission times configuration takes effect only for the HTTP connections pushed by an iPortal page.

Configuration Steps

Configuring the iPortal HTTP Retransmission Times

- Set a parameter in global configuration mode.

Command	**iportal retransmit** *count*
Parameter Description	*count*: Indicates the retransmission times.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Send an iPortal Web authentication request and disconnect from the network. Check whether the NAS resends an HTTP connection request.

Configuration Example

Configuring the Retransmission Times

Configuration Steps	● Configure the retransmission times.
	Ruijie(config)#iportal retransmit 5
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure the retransmission times.
	`Ruijie(config)#iportal retransmit 5`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `iportal retransmit 5`

1.4.33. Configuring Service Selection in Ruijie iPortal Web Authentication

Configuration Effect

- Configure the service type used by Ruijie iPortal Web Authentication.

Notes

- N/A

Configuration Steps

Configuring the Service Type Used by Ruijie iPortal Web Authentication

- Configure a service type in global configuration mode.

Command	**iportal service [internet** *internet-name***] [local** *local-name* **]**
Parameter Description	*internet-name*: Indicates the external service name to be used. *local-name*: Indicates the internal service name to be used.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring a Service Type

Configuration Steps	● Configure a service type.
	`Ruijie(config)#iportal service local local-srv`
Verification	● Check whether the configuration is successful.

Configuration Steps	● Configure a service type.
	`Ruijie(config)#iportal service local local-srv`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `iportalservice local local-srv`

1.4.34. Configuring the Accounting Method List of Web Authentication

Configuration Effect

- Configure Web authentication accounting methods based on different templates.

Notes

- If no accounting method is configured for Web authentication, the default method is used.

Configuration Steps

↘ Configuring an Accounting Method

- Configure an accounting method in global or template configuration mode.

Command	**web-auth accounting v2 { default |** *name* **}**
Parameter Description	*name*: Indicates the name of the accounting method list to be used.
Command Mode	Global or template configuration mode
Usage Guide	N/A

Verification

- View the destination IP address of accounting packets.

Configuration Example

↘ Configuring an Accounting Method

Configuration Steps	● Configure an accounting method.

	`Ruijie(config.tmplt.eportalv2)#web-auth accounting v2 default`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config` `...` `web-auth accounting v2 default`

1.4.35. Configuring a Web Authentication Method List

Configuration Effect

- Configure Web authentication methods based on different templates.

Notes

- If no Web authentication method is configured, the default method is used.

Configuration Steps

↘ Configuring a Web Authentication Method List

- Configure a Web authentication method in global or template configuration mode.

Command	**web-auth authentication v2 { default |** *name* **}**
Parameter Description	*name*: Indicates the name of the Web authentication method list to be used.
Command Mode	Global or template configuration mode
Usage Guide	N/A

Verification

- View the destination IP address of authentication packets.

Configuration Example

↘ Configuring a Web Authentication Method

Configuration Steps	● Configure a Web authentication method.
	`Ruijie(config.tmplt.eportalv2)#web-auth authentication v2 default`

Verification	• Check whether the configuration is successful.
	Ruijie(config)#show running-config ... web-auth authentication v2 default

1.4.36. Customizing a Page Suite

Configuration Effect

- Customize a webpage to display logos or advertisements in Ruijie iPortal Web Authentication.
- A single page suite supports two page sets to adapt to the screen sizes of STAs, for example, mobile STAs with a small screen.

Notes

- The preparation of a page suite must comply with the relevant specification; otherwise, the customized page suite cannot be used.
- The maximum number of files in a page suite (including the files displayed on PCs and mobile STAs) is 50, and the maximum length of the file name of each page is 32 bytes.
- A new page suite must be downloaded to the ./portal directory and the name must not be the same as that of the default page suite; otherwise, the default page suite will be overwritten.
- Some NASs do not have a default page suite. When Ruijie iPortal Web Authentication is implemented, prepare a page suite in accordance with the relevant specification and import the page suite to the flash memory.

Verification

- Simulate the scenario where an STA connects to the Internet and opens the browser to perform authentication. Check that the customized page is displayed.

Related Commands

↘ Page File Naming Specification

Page File Name (with an Extension)	Usage
login.htm	Login page
online.htm	Online page (which is displayed when users pass authentication)
offline.htm	Offline page
login_mobile.htm	Login page for mobile STAs
online_mobile.htm	Online page for mobile STAs (which is displayed when users pass authentication)

offline_mobile.htm	Offline page for mobile STAs

Login Page Preparation Specification

According to the page file naming specification, the file name of the login page for PCs is login.htm, and that for mobile STAs is login_mobile.htm. The login page content specification is described in the following.

- Form elements

The login page must contain a form, and the form submission method is fixed to POST. The PC login page is used as an example. Assume that the PC login page is stored in the **/portal** directory. The HTML code of the form is as follows (the HTML code of the form of the mobile STA login page is similar):

```
<form method="post" action="/portal/login.htm">
...
</form>
```

The form of the login page must contain the following page elements:

1. (Mandatory) **User name** text box: allows a user to enter the user name. The text box ID is username.
2. (Mandatory) **Password** text box: allows a user to enter the password (which is not displayed in plaintext mode). The text box ID is password.
3. (Mandatory) **Login** button: allows a user to submit a form using the POST method.
4. (Optional) Tab showing an authentication failure cause: The ID of the tab is errormsg. The tab is displayed on the login page to show why the current user fails authentication. When the login page is loaded, an error message request is sent using the GET method, and the request results will be displayed on the errormsg tab. You can configure whether to display the errormsg tab on the login page as required. The following script is used to request the error message content from the server (the script is only one example):

```
< script language=”javascript”>
//Request the error message content from the server.
function requestErrorMsg() {
    var _errormsg=document.getElementById(“errormsg”);
     var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
}

//Call the init function when the login page is loaded.
function init() {
……
```

requestErrorMsg();

}

……

</script>

- Form submission

A form is submitted in the format of username=[AAAA]&password=[BBBB]&lang=[CCCC]. The meanings of the fields are described in the following:

[AAAA]: (optional)Indicates the user name that the user enters in the **User name** text box.

[BBBB]: (optional)Indicates the password that the user enters in the **Password** text box.

[CCCC]: (optional) Indicates the language environment. The value **1** indicates Simplified Chinese, and the value **2** indicates English. Other languages are not defined. The default language environment is Simplified Chinese. When English is used, the submitted form must contain the language environment information; otherwise, the content of the errormsg tab is in Chinese.

The form of the login page must contain at least the following three input fields (tabs): **username**, **password**, and **Login** button. If the login page provides the Chinese and English language options, the form may also contain the **Language** input field, which is invisible.

The HTML source code of the login page is as follows:

<html>

<head>

<title>Web authentication login page</title>

</head>

<script language=”javascript”>

//Request errormsg. Errormsg is empty and not displayed when a user passes authentication or the login page is loaded for the first time.

function requestErrorMsg() {

var _errormsg=document.getElementById(“errormsg”);

var script=document.createElement(“script”);

script.src=”errormessage”+location.search;

_errormsg.appendChild(script);

}

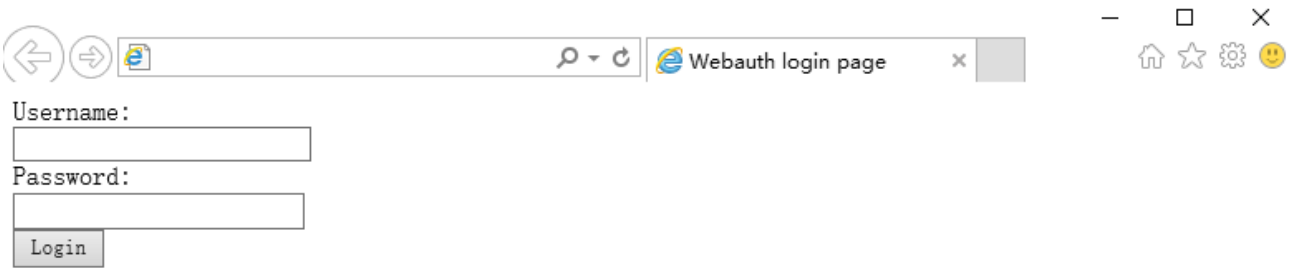
function init() {

……

requestErrorMsg();

```
}

//Script that is executed when a user clicks the Login button
function login() {
   document.getElementById('loginForm').action = "./login.htm"+location.search;
       document.getElementById('loginForm').submit();
       window.onbeforeunload = null;
       window.onunload = null;
}
……

</script>
<body onload="init()">
<form method="post" id=”loginForm”>
User name:<br>
<input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
<br>
Password:<br>
<input type="password" name="password" accesskey="p" size="25"
            value="" id="password">
<br>
<input type="button" onclick=”login()” value="Login" id=”loginButton”>
<input type="hidden" name="lang" value="" id="lan">
       <p name=”errormsg” id="errormsg"></p>
</form>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users:



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Online Page Preparation Specification

The online page is designed to inform a user that the user has passed authentication and can use network resources normally. The file name of the login page for PCs is **login.htm**, and that for mobile STAs is **login_mobile.htm**.

- Form elements

The online page must contain a form, which is used to submit an offline request. For this reason, the form must contain a **Logout** button. The form submission method is fixed to POST. The PC online page is used as an example. Assume that the PC online page is stored in the **/portal** directory. The HTML code of the form is as follows (the HTML code of the form of the mobile STA online page is similar):

```
<form method="post" action="/portal/online.htm">
...
</form>
```

The form of the online page must contain the following page elements:

1. (Optional) Tab with the username ID: displays the information of the online user.
2. (Optional) Tab with the userip ID: displays the IP address of the online user.
3. (Optional) Tab with the usermac ID: displays the MAC address of the online user.
4. (Optional) Tab with the ssid ID: displays the SSID of the online user.
5. (Optional) Tab with the availtime ID: displays the available time during which the user can access the Internet.
6. (Mandatory) **Logout** button: allows the user to go offline and requests the display of the offline page.

When the online page is loaded, a request is sent using the GET method to retrieve user information from the server, including the user name, IP address, MAC address, and associated SSID of the online user, and available time. The URI is getonlineinfo. The onload method of the body in the HTML code must be used. The following script is used to request user information from the server (the script is only one example):

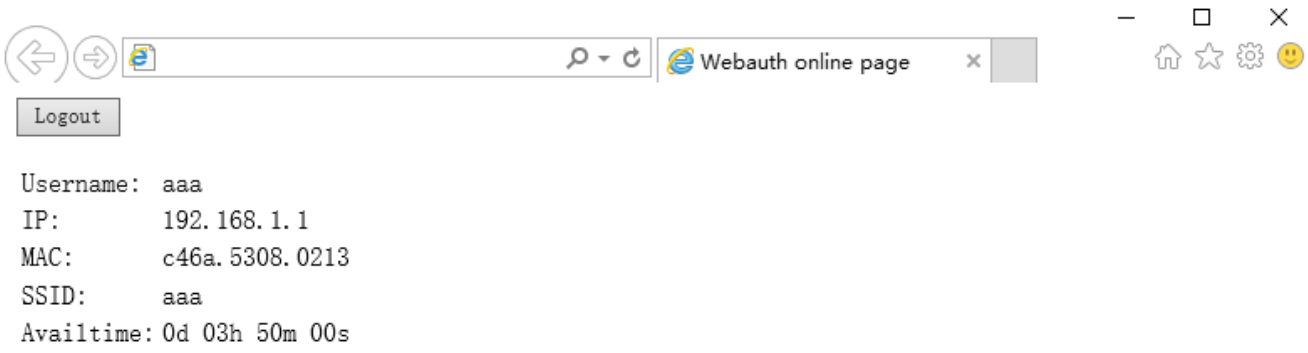
```
<script language="javascript">
//Obtain the information of the online user, including the user name, IP address, MAC address, and associated SSID of the online user, and available time.
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
    }
</script>
<body onload="init()">
……
</body>
```

The HTML source code of the online page is as follows:

```
<html>
<head>
<title>Web authentication online page</title>
</head>
<script language="javascript">
//Obtain the information of the online user, including the user name, IP address, MAC address, and associated SSID of the online user, and available time.
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo ();
    }
    //Script that is executed when the user clicks the Logout button. The request URI is offline.htm.
```

```
    function logout() {
        document.logoutform.action = "./offline.htm"+location.search;
        document.logoutform.submit();
        window.onbeforeunload = null;
         window.onunload = null;
    }

</script>

<body onload="init()">
<form method="post" action="/portal/offline.htm" id="logoutform">
<input type="button" onclick="logout()" value="Logout" id="logoutButton">
</form>
    <table>
    <tr><td>User name:</td><td id="username"></td></tr>
    <tr><td>IP address:</td><td id="userip"></td></tr>
    <tr><td>MAC address:</td><td id="usermac"></td></tr>
    <tr><td>Associated SSID:</td><td id="ssid"></td></tr>
    <tr><td>Available time:</td><td id="availtime"></td></tr>
    </table>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users:



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

↘ Offline Page Preparation Specification

The offline page is displayed when a user clicks the **Logout** button on the online page. The offline page is designed to inform the user that the user logs out successfully. If the user needs to access the Internet after logout, the user must perform authentication. The file name of the offline page for PCs is **offline.htm**, and that for mobile STAs is **offline_mobile.htm**.

The offline page has the following elements:

1. (Optional) Tab with the timeused ID: displays the time that has used by the user to access the Internet.

When the offline page is loaded, a request is sent using the GET method to retrieve the used-time information from the server. The request URI is getofflineinfo. The onload method of the body in the HTML code must be used. To obtain the used-time information, you can create a dynamic script. For example, you can create **script.src=" getofflineinfo"** to include the field information to be sent in the **src** of the script. The following script is used to request the used-time information from the server (the script is only one example):

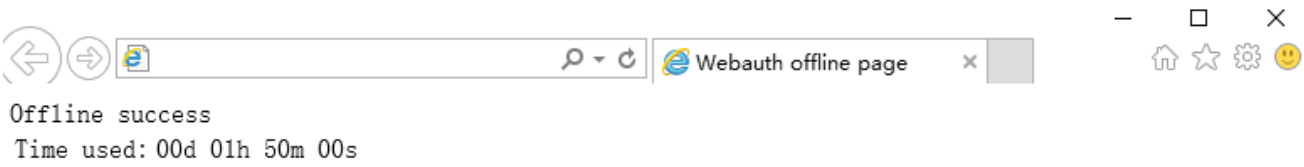
```
<script language="javascript">
//Obtain the used time information.
    function requestOfflineInfo() {
    var _timeused =document.getElementById("timeused");
        var script=document.createElement("script");
        script.src="getofflineinfo"+location.search;
     _timeused.appendChild(script);
     }

     function init() {
          requestUserInfo();
     }
</script>
<body onload="init()">
……
</body>
```

The HTML source code of the offline page is as follows:

```
<html>
<head>
<title>Web authentication offline page</title>
</head>
<script language="javascript">
//Obtain the used time information.
    function requestOfflineInfo() {
          var _timeused=document.getElementById("timeused");
```

```
            var script=document.createElement("script");
            script.src="getofflineinfo"+location.search;
            _timeused.appendChild(script);
    }

    function init() {
        requestOfflineInfo();
    }
</script>

<body onload="init()">
Logout succeeded<br>
 <table>
 <tr><td>Used time:</td><td id="timeused"></td></tr>
 </table>
</body>
</html>
```

The following figure shows the offline page that the iPortal server pushes to users:

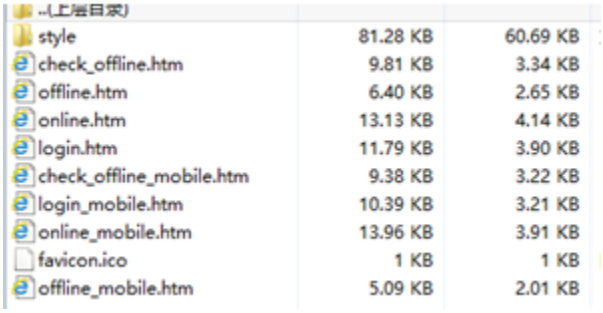


The offline page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Page Compression Specification

After you prepare the login page, online page, and offline page in accordance with the specification described above, you need to compress the pages and related elements and upload them to the NAS. Then you can apply the page suite. The page compression specification is as follows:

1. Compress the prepared pages and related element files (such as image files and style sheet files) into a **.zip** package, for example, **portal1_page.zip**.
2. You can create directories in a page suite. For example, the **portal1_page.zip** package shown in the following figure has the **style** directory, which contains the CSS files of pages and other image files.



style	81.28 KB	60.69 KB
check_offline.htm	9.81 KB	3.34 KB
offline.htm	6.40 KB	2.65 KB
online.htm	13.13 KB	4.14 KB
login.htm	11.79 KB	3.90 KB
check_offline_mobile.htm	9.38 KB	3.22 KB
login_mobile.htm	10.39 KB	3.21 KB
online_mobile.htm	13.96 KB	3.91 KB
favicon.ico	1 KB	1 KB
offline_mobile.htm	5.09 KB	2.01 KB

After you compress the pages into a page suite, use TFTP or other tools to upload the page suite to the**/portal/zip/** directory of the flash memory on the NAS. Then configure the portal server to use the page suite (that is, associate the portal server with the page suite). For details, see the configuration manual related to Web authentication. A directory named after the page suite package is created in the/portal/ext_zip/ directory of the flash memory. For example, if the page suite package is named **portal1_page.zip**, the**/portal/ext_zip/protal1_page/** directory of the flash memory is created, and the package is automatically decompressed in the directory. The portal server can push Web authentication pages to users based on the page suite.

Configuration Example

↘ Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	`Ruijie(config.tmplt.iportal)#page-suit ruijiepage`
Verification	● Check whether the configuration is successful.
	`Ruijie#show web-auth template` `Webauth Template Settings:` `----------` `Name: iportal` `Page-suit: ruijiepage` `Advertising url: default`

Configuration Steps	● Customize a page suite.
	`Ruijie(config.tmplt.iportal)#page-suit ruijiepage`
Verification	● Check whether the configuration is successful.
	`Advertising mode: online-popup` `Type: Intral Portal` `Acctmlist:default` `Authmlist:default`

1.4.37. Upgrade Compatibility

Configuration Effect

- Some configuration commands are optimized in the 11.X series software and the command formats are changed. For details, see the subsequent description.
- The 10.X series software supports smooth upgrade without function loss. However, some commands are displayed in new formats after upgrade.
- When you run the commands in earlier formats in the **no** form in the 11.X series software, a message is displayed, indicating the **no** form is not supported. You need to perform the **no** operation in new command formats.

Configuration Steps

- It is recommended that you run commands in new formats.

Verification

- Check that function loss does not occur when the 10.X series software is upgraded to the 11.X series software, and commands are displayed and stored in new formats.
- The commands in new formats have the same functions as the commands in earlier formats.

Related Commands

↘ **Configuring the IP Address of the Portal Server in Ruijie First-Generation Web Authentication**

Command	**http redirect** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of the ePortal server in Ruijie First-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 template, and the **ip** command in template configuration mode is executed to configure and display the IP address of the portal server. For details, see

	section 1.4.1"Configuring Ruijie First-Generation Web Authentication."

Configuring the Portal Server

Command	**portal-server [eportal1 | eportalv2]**
Parameter Description	**eportav1**: Indicates the information of the portal server used in Ruijie First-Generation Web Authentication. **eportav2**: Indicates the information of the portal server used in Ruijie Second-Generation Web Authentication.
Command Mode	Global configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 or eportalv2 template, and relevant information is filled in. The main parameters of the portal server include the IP address and URL of the server. The original command will be replaced by the **ip** command and **url** command in the template.

Configuring Web Authentication Control on a Port

Command	**web-auth port-control**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In the 11.X version, the command is converted into **web-auth enable <type>**, in which **type** specifies the type (first or second generation) of Web authentication. The default type is Ruijie First-Generation Web Authentication.

Configuring the IP-Only Binding Mode

Command	**web-auth port-control ip-only-mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In the 11.X version, the command is converted into an eportalv1 or eportalv2 template, depending on the actual configuration. The server binding mode is configured and displayed by using the **bindmode** command in template configuration mode. For details, see section 1.4.1 "Configuring Ruijie First-Generation Web Authentication" and section 1.4.2 "Configuring Ruijie Second-Generation Web Authentication."

Configuring VLAN-Based Web Authentication

Command	**web-auth allow-vlan** *list*
Parameter Description	*list*: Indicates the list of VLANs for which Web authentication is enabled.
Command Mode	Global configuration mode

Usage Guide	In the 11.X version, the command is converted into a command used to configure VLAN-based SCC authentication exemption.

Displaying the Configuration Information of Ruijie First-Generation Web Authentication

Command	**show http redirect**
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth template**.

Displaying the Port Control Information

Command	**show web-auth port-control**
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	In the 11.X version, the command is unavailable and changed to **show web-auth control**.

Configuration Example

Configuring Ruijie First-Generation Web Authentication

Configuration Steps	● Check that the NAS runs on the 10.X version and is configured with the IP address of the portal server used by Ruijie First-Generation Web Authentication.
	`Ruijie(config)# http redirect 192.168.197.64`
	● Upgrade the NAS to 11.X.
Verification	● Run the **show running-config** command after the upgrade and check whether the new command formats are used.
	`Ruijie#sh running-config` `web-auth template eportalv1` `  Ip 192.168.197.64` `!`

1.4.38. Configuring Noise Reduction in Wireless Web Authentication

Configuration Effect

- When the number of times an STA accesses an IP address reaches the configured threshold, the subsequent packets that the STA sends to the IP address will be dropped, in order to realize noise reduction.

Notes

- Configure the two parameters (aging time and hit times) for noise reduction based on the network condition and actual requirements to avoid the dropping of normal packets, which will affect redirection.

Configuration Steps

Configuring Noise Reduction in Global Configuration Mode

Command	**web-auth noise**[**aging** *agmin*] [**hit** *times*]
Parameter Description	*agmin*: Indicates the aging time of noise reduction. The default value is 1 minute. *times*: Is a rule of noise reduction. When the number of times an STA accesses an IP address reaches the threshold specified by the *times* parameter, noise is considered to occur. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Simulate the scenario where an STA accesses an IP address repeatedly during redirection until the maximum number of access times is reached. Check whether the subsequent packets that the STA sends to the IP address are redirected or not. After the aging time of the noise reduction has elapsed, check whether the packets that the STA sends to the IP address are redirected again.

Configuration Example

Configuring Noise Reduction in Wireless Web Authentication

Configuration Steps	- Set the parameters of noise reduction in wireless Web authentication. `Ruijie(config)#web-auth noise aging 1 hit 3`
Verification	- Check whether the configuration is successful. `Ruijie(config)#show running-config`

1.4.39. Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication

Configuration Effect

- Enable iOS STAs to support the automatic display of pop-up windows and display Wi-Fi signal reception during WeChat-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). (iOS STAs can use the WeChat app without login when the WeChat traffic straight-through function is enabled.)

Notes

- iOS automatic pop-up window control must be used together with the WeChat traffic straight-through function (run the web-ctrl free-auth weixin command to enable this function).
- The redirection performance will be reduced after iOS automatic pop-up window control is enabled.
- iOS automatic pop-up window control will be invalid when the straight-through function is enabled for the Apple Inc. website by running the following commands:
- web-ctrl free-auth iphone
- web-auth acl white-url http://www.apple.com.cn
- web-auth acl white-url http://captive.apple.com

Configuration Steps

Enabling iOS Automatic Pop-up Window Control in Global Configuration Mode

Command	**http redirect adapter ios**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Check that iOS STAs show pop-up windows and display Wi-Fi signal reception during WeChat-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). (iOS STAs can use the WeChat app without login when the WeChat traffic straight-through function is enabled.)

Configuration Example

Enabling iOS Automatic Pop-up Window Control in WeChat-Based Authentication

Configuration Steps	• Enable iOS automatic pop-up window control. `Ruijie(config)#http redirect adapter ios`
Verification	• Check whether the configuration is successful. `Ruijie(config)#show running-config`

1.4.40. Enabling the Smart WeChat Web Authentication

Configuration Effect

- When an STA is associated with an SSID for the second time during WeChat Web authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication), the STA gets online without authentication.

Notes

- You need to run the ip dhcp snooping command before the smart authentication function takes effect.

Configuration Steps

Configuring the Smart Authentication in Global Configuration Mode

Command	**web-auth sta-perception enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Simulate the scenario where an STA is associated with an SSID for the second time during WeChat Web authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). Check whether the STA gets online without authentication.

Configuration Example

Enabling the Smart WeChat Web Authentication

Configuration Steps	• Enable the smart WeChat Web authentication. • The configuration is optional.
	`Ruijie(config)#web-auth sta-perception enable`
Verification	• Check whether the configuration is successful.
	`Ruijie(config)#show running-config`

1.4.41. Configuring User Detection Under WLANSEC

Configuration Effect

- After online user detection under WLANSEC is configured, if the traffic of a user is lower than the threshold within a specified interval, the device automatically forces the user to go offline, to prevent economic loss for the user due to continuous charging.

Notes

- The function has the same effect as the SCC command executed in global configuration mode: **offline-detect interval** *interval* thredshold *thredshold*. The configuration of user detection under WLANSEC has a higher priority than the SCC command executed in global configuration mode.

Configuration Steps

- (Optional) By default, a user is forced to go offline if there is no traffic of the user within 15 minutes.

If **flow** is set to **0**, traffic detection is not performed.

By default, traffic detection under WLANSEC is disabled in 10.X version and the global configuration is used. After the version is upgraded to 11.X, traffic detection under WLANSEC needs to be manually disabled.

Verification

- After online user detection is configured, enable a user to go online, shut down the specified authenticated terminal, and wait for the specified interval to elapse. Then, run the **show web user** command on the device to check that the user has gone offline.

Related Commands

Configuring User Detection Under WLANSEC

Command	**web-auth offline-detect interval** *interval* **flow** *thredshold* **no web-auth offline-detect** **default web-auth offline-detect**
Parameter Description	*interval*: Indicates the offline detection interval. The value ranges from 1 min to 65535 min. The default value is 15 min. *thredshold*: Indicates the traffic threshold. The value ranges from to 0 bytes to 4294967294 bytes. The default value is 0, indicating that traffic detection is not performed. **no web-auth offline-detect**: Disables online user detection. **default web-auth offline-detect**: Restore the default value. That is, authenticated online users are forced to go offline if their traffic is zero within 15 min.
Defaults	15 min
Command Mode	WLANSEC configuration mode
Usage Guide	This command can be used to configure the online keepalive time for users. Authenticated online users are

	forced to go offline if their traffic is lower than the specified threshold within a specified interval.

Configuration Example

Configuring User Detection Under WLANSEC

Configuration Steps	● Set user detection under WLANSEC 1.
	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#web-auth offline-detect interval 30 flow 10000`
Verification	● Check whether the configuration is successful.
	`Ruijie(config)#show running-config | be wlansec 1` `wlansec 1` `  web-auth offline-detect interval 30 flow 10000` `...`

1.4.42. Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol

Configuration Effect

- Configure transparent transmission of the 0x05 attribute of the portal protocol. After this function is enabled, the Web authentication server supports transparent transmission of the 0x05 attribute in the following scenarios:
  1. When the portal protocol of China Mobile is interworked, the Web authentication server encapsulates the error flag into the 0x05 attribute (ErrID) and transparently transmits it to the portal server.
  2. When Huawei portal protocol 2.0 is interworked, the Web authentication server encapsulates prompts from third-party authentication device such as the RADIUS server to the 0x05 attribute (TextInfo) and transparently transmits them to the portal server.

Notes

- This function is disabled by default.

Configuration Steps

- Optional.
- Configure this function when the ErrID (0x05) attribute specified in the portal protocol of China Mobile is required.
- Configure this function when the TextInfo (0x05) attribute specified in Huawei portal protocol 2.0 is required.

Related Commands

Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol in Global Configuration Mode

Command	**web-auth portal-attribute 5**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, enable this function on the portal server when a device needs to upload the error flag (ErrID).
Command	**web-auth portal-attribute textinfo**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, enable this function on the portal server (using Huawei portal protocol 2.0) when a device needs to upload prompts (TextInfo) from a third-party authentication device such as the RADIUS server.

Verification

- After this function is enabled, check that the 0x05 attribute is contained in the ACK packet responded to the portal server.

Configuration Example

Configuring Transparent Transmission of the 0x05 Attribute of the Portal Protocol

Configuration Steps	• Configure transparent transmission of the 0x05 attribute.
	`Ruijie(config)# web-auth portal-attribute 5` `Or:` `Ruijie(config)# web-auth portal-attribute textinfo`
Verification	• Check whether the configuration is successful.
	`Ruijie(config)#show running-config`

1.4.43. Configuring Uniqueness Check of Portal Authentication Accounts

Configuration Effect

- Configure the uniqueness check of portal authentication accounts. After this function is enabled, the Web authentication server checks account information in the user authentication request. If finding that the account has been used by another user and is online, the Web authentication server directly responds to the portal server with ErrCode 2-contained ACK_AUTH. After receiving such response, some portal servers push the "Terminal Preemption" prompt to users.

Notes

- This function is disabled by default.

Configuration Steps

- Optional.
- Configure the function when the portal server needs to push the "Terminal Preemption" prompt to users.

Related Commands

Configuring Uniqueness Check of Portal Authentication Accounts in Global Configuration Mode

Command	**web-auth portal-valid unique-name**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	In general, configure the function when the portal server needs to push the "Terminal Preemption" prompt to users.

Verification

- After this function is enabled, if finding that a same account is used by another user and is online, the Web authentication server directly responds to the portal server with ErrCode 2-contained ACK_AUTH.

Related Commands

Configuring Uniqueness Check of Portal Authentication Accounts

Configuration Steps	• Configure uniqueness check of portal authentication accounts.
	`Ruijie(config)# web-auth portal-valid unique-name`
Verification	• Check whether the configuration is successful.
	`Ruijie(config)#show running-config`

Configuration Steps	● Configure uniqueness check of portal authentication accounts.
	`Ruijie(config)# web-auth portal-valid unique-name`
Verification	● Check whether the configuration is successful.

1.4.44. Enabling the One-click Configuration via WiFiDog

Configuration Effect

- Use one command to configure WiFiDog template information, port control, global survival, iOS window display, and imperceptible authentication.

Notes

- The **no** form of this command can delete template information and controlled ports, but is not globally valid.

Configuration Steps

↘ Enabling the One-click Configuration via WiFiDog

- Optional.

Command	**web-auth wifidog-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip** *nas-ip-address* **url** *url-string* **[gateway-id** *gwid-string* **]** [**perception**]
Parameter Description	*name*: Indicates the template name. *Intf:* Indicates the controlled interface. *portal-ip-addr*: Indicates the IP address of the portal server. *nas-ip-addr:* Sets the IP address for a device with WiFiDog configured to access a service, so that the server sends packets to this IP address for communication. *url-string:* Indicates the URL for portal server authentication. *gwid-string*: Indicates the gateway ID. It is mandatory to configure it only in scenarios of hot backup or VAC. **perception**: Configures the imperceptible authentication function.
Command Mode	Global configuration mode
Usage Guide	The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.

Verification

- Run the **Show run** command to check whether the configuration is normal.

Configuration Example

Enabling the One-click Configuration via WiFiDog

Configuration Steps	● Enable the one-click configuration via WiFiDog.
	`Ruijie(config)# web-auth wifidog-template aaa interface tenGigabitEthernet 3/2 portal-ip 172.21.6.78 nas-ip 192.168.197.227 url http://172.21.6.78/auth/wifidogAuth`
Verification	● Run the **show running-config** command to check whether the configuration is successful.

1.4.45. Enabling the One-click Configuration via WeChat

Configuration Effect

- Use one command to configure WeChat template information, port control, global survival, PC free authentication, iOS window display, and imperceptible authentication.

Notes

- The **no** form of this command can delete template information and controlled ports, but is not globally valid.

Configuration Steps

Enabling the One-click Configuration via WeChat

- Optional.

Command	**web-auth wechat-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip nas-ip-address [nas-id** *nas-id-string***]** [**perception** | **ios-adapter**]
Parameter Description	*name*: Indicates the template name. *Intf:* Indicates the controlled interface. *portal-ip-addr*: Indicates the IP address of the portal server. *nas-ip-addr:* Sets the IP address for a device with WeChat configured to access a service, so that the server sends packets to this IP address for communication. *nas-id-string*: Indicates the NAS ID of the device. The default NAS ID is the MAC address of the master AC. It has to be configured in scenarios of hot backup or VAC. **perception**: Configures the imperceptible authentication function. **ios-adapter**: Configures the automatic window display function.
Command Mode	Global configuration mode
Usage Guide	The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.

Verification

- Run the **Show run** command to check whether the configuration is normal.

Configuration Example

Enabling the One-click Configuration via WeChat

Configuration Steps	• Enable the one-click configuration via WeChat.
	`Ruijie(config)# web-auth wechat-template aaa interface tenGigabitEthernet 3/2 portal-ip 172.21.6.78 nas-ip 192.168.197.227`
Verification	• Run the **show running-config** command to check whether the configuration is successful.

1.4.46.Configuring NAS-PORT-ID for an AP

Configuration Effect

- The China Mobile, Guangdong branch requires that the **NAS-PORT-ID** parameter be configured for each AP. After the parameter is configured, the parameter will be sent to the portal and Radius severs using portal and radius packets, respectively.

Notes

- The **NAS-PORT-ID** parameter can be configured only for single APs.

Configuration Steps

Configuring NAS-PORT-ID for an AP

- Optional.

Command	**nas-port-id** *string*
Parameter Description	*string*: NAS-PORT-ID name allocated to an AP.
Command Mode	AP configuration mode
Usage Guide	This command sets the **NAS-PORT-ID** parameter only for single APs. To cancel configuration, run the **no nas-port-id** command.

Verification

- Run the **show ap-config running** command to check whether the configuration is normal.

Configuration Example

Configuring NAS-PORT-ID for an AP

Configuration Steps	● Configure the **NAS-PORT-ID** parameter.
	`Ruijie(config)# ap-config ap740` `Ruijie(config-ap)# nas-port-id guangdongyidong`
Verification	● Run the **show ap-config running** command to check whether the configuration is successful.

1.4.47.Enabling Automatic Adding of Domain Information After Usernames

Configuration Effect

- When Ruijie Second-Generation Web Authentication or Ruijie Internal Portal (iPortal) Web Authentication is applied, run the **domain** *domain-string* command to automatically add domain information after original usernames. Then the new usernames are sent to the AAA server.

Notes

- Up to 63 bytes are supported in the domain information. If the combination of the original username and the domain information exceeds 253 bytes, the excessive part of the domain information is removed.

Configuration Steps

- Optional.
- This feature is supposed to be configured when automatic adding of domain information is not supported on the Portal server but the Radius server requires domain information.

Verification

- Run the **show running-config** command to check if the command is properly configured.

Related Command

↘ Enabling Automatic Adding of Domain Information After Usernames

Command	**domain** *domain-string*
Parameter Description	*domain-string*: A string indicating domain information.
Command Mode	Web authentication configuration mode
Usage Guide	For example, if the original username sent from the Portal server is ruijie, and the string is set to @wifi, then the new username sent to the AAA server is ruijie@wifi.

Configuration Example

↘ Enabling Automatic Adding of Domain Information After Usernames

Configuration Steps	● Configure “@wifi” as the domain information for the eportalv2 template.
	`Ruijie(config.tmplt.eportalv2)#domain @wifi`
Verification	● Run the **show run** command to check whether the configuration is successful.
	`Ruijie(config)#show run` `web-auth template eportalv2` `domain @wifi` `Ruijie(config)#`

1.5. Monitoring

Clearing

Description	Command
Forces users offline.	**clear web-auth user** { **all | ip** *ip-address* | **mac** *mac-address* **| name** *name-string* **| session-id** *num* }
Clears all the straight-through network resources.	**clear web-auth direct-site**
Clears all the authentication-exempted users.	**clear web-auth direct-host**
Clears the Webauth blacklist and whitelist configuration.	**clear web-auth acl**

Displaying

Description	Command
Displays the Webauth blacklist and whitelist configuration.	**show web-auth acl**
Displays the basic parameters of Web authentication.	**show web-auth parameter**
Displays the Webauth template configuration.	**show web-auth template**
Displays the authentication-exempted host range.	**show web-auth direct-host**
Displays the straight-through address range.	**show web-auth direct-site**

Description	Command
Displays the straight-through ARP range.	**show web-auth direct-arp**
Displays the TCP interception port.	**show web-auth rdport**
Displays the Webauth configuration on a port.	**show web-auth control**
Displays the online information of all users or specified users.	**show web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* | **escape** | **by-ap** *ap-name* | **by-ap-group** *ap-group-name* }
Displays the Webauth CGI configuration.	**show web-auth cgi**
Displays the basic global Webauth information.	**show web-auth global**
Displays the global Webauth template.	**show web-auth global authentication**
Displays the customized Webauth page suite.	**show web-auth global customized-pages**
Displays the iPortal server information.	**show web-auth global local-portal**
Displays the global Webauth template.	**show web-auth global template**
Displays the global Webauth type.	**show web-auth global webauth-type**
Displays the Webauth configuration.	**show web-auth info**
Displays the iPortal Webauth information.	**show web-auth local-portal**
Displays the Webauth portal check information.	**show web-auth portal-check**
Displays the noise reduction configuration of Web authentication.	**show web-auth noise**

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs Web authentication.	**debug web-auth all**

2 Configuring AAA

2.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring the authentication, authorization, and accounting services. Ruijie Networks devices support the AAA application.

AAA provides the following services in a modular way:

Authentication: Refers to the verification of user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+).

Authorization: Refers to the granting of specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe what operations users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.

Accounting: Refers to the tracking of the resource consumption of users. When accounting is enabled, NASs collect statistics on the network resource usage of users and send them in AV pairs to authentication servers. The records will be stored on authentication servers, and can be read and analyzed by dedicated software to realize the accounting, statistics, and tracking of network resource usage.

AAA is the most fundamental method of access control. Ruijie Networks also provides other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher level of network security.

AAA has the following advantages:

- Robust flexibility and controllability
- Scalability
- Standards-compliant authentication
- Multiple standby systems

2.2 Applications

Application	Description
Configuring AAA in a Single-Domain Environment	AAA is performed for all the users in one domain.
Configuring AAA in a Multi-Domain Environment	AAA is performed for the users in different domains by using different methods.

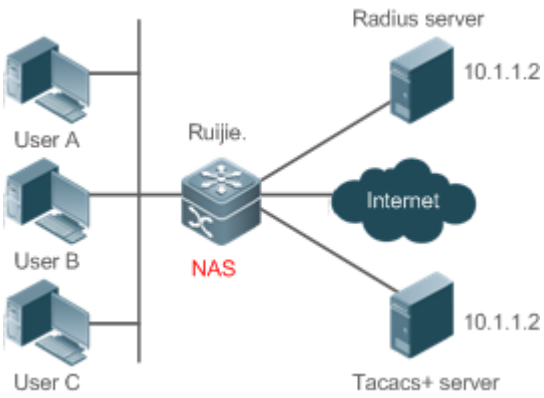
2.2.1 Configuring AAA in a Single-Domain Environment

Scenario

In the network scenario shown in Figure 2-1, the following application requirements must be satisfied to improve the security management on the NAS:

3. To facilitate account management and avoid information disclosure, each administrator has an individual account with different username and password.
4. Users must pass identity authentication before accessing the NAS. The authentication can be in local or centralized mode. It is recommended to combine the two modes, with centralized mode as active and local mode as standby. As a result, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, it turns to local authentication.
5. During the authentication process, users can be classified and limited to access different NASs.
6. Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
7. The AAA records of users are stored on servers and can be viewed and referenced for auditing. (The TACACS+ server in this example performs the accounting.)

Figure 2-1



Remarks	User A, User B, and User C are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor. The TACACS+ server can be the dedicated server software provided by a vendor.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure the authentication service on the NAS.

- Configure the authorization service on the NAS.
- Configure the accounting service on the NAS.

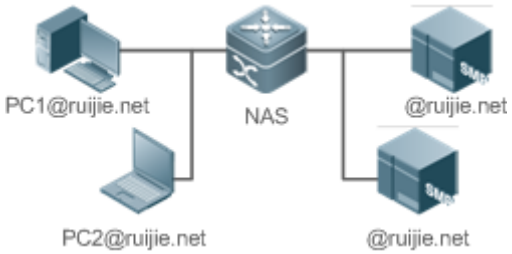
2.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username PC1@ruijie.net or PC2@ruijie.com.cn and correct password on an 802.1X client.
- Permission management: Users managed are classified into Super User and Common User. Super users have the rights to view and configure the NAS, and common users are only able to view NAS configuration.
- The AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 2-2



Remarks	The clients with the usernames **PC1@ruijie.net** and **PC2@ruijie.com.cn** are connected to the NAS in wired or wireless way. The NAS is an access or convergence switch. The Security Accounts Manager (SAM) server is a universal RADIUS server provided by Ruijie Networks.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Define an AAA method list on the NAS.
- Enable domain-based AAA on the NAS.
- Create domains and AV sets on the NAS.

2.3 Features

Basic Concepts

↘ **Local Authentication and Remote Server Authentication**

Local authentication is the process where the entered passwords are verified by the database on the NAS.

Remote server authentication is the process where the entered passwords are checked by the database on a remote server. It is mainly implemented by the RADIUS server and TACACS+ server.

Method List

AAA is implemented using different security methods. A method list defines a method implementation sequence. The method list can contain one or more security protocols so that a standby method can take over the AAA service when the first method fails. On Ruijie devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a security method responds or all the security methods in the list are tried out. Authentication fails if no method in the list responds.

A method list contains a series of security methods that will be queried in sequence to verify user identities. It allows you to define one or more security protocols used for authentication, so that the standby authentication method takes over services when the active security method fails. On Ruijie devices, the first method in the list is tried in the beginning and then the next is tried one by one if the previous gives no response. This method selection process continues until a method responds or all the methods in the method list are tried out. Authentication fails if no method in the list responds.

The next authentication method proceeds on Ruijie devices only when the current method does not respond. When a method denies user access, the authentication process ends without trying other methods.

Figure 2-3

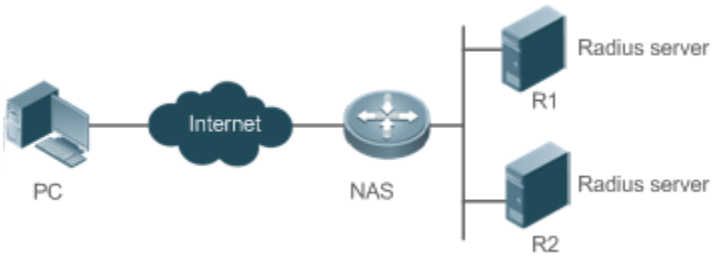


Figure 2-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

Assume that the system administrator defines a method list, where the NAS selects R1 and R2 in sequence to obtain user identity information and then accesses the local username database on the server. For example, when a remote PC user initiates dial-up access, the NAS first queries the user's identity on R1. When the authentication on R1 is completed, R1 returns an Accept response to the NAS. Then the user is permitted to access the Internet. If R1 returns a Reject response, the user is denied Internet access and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query.

When detecting a timeout event, the AAA service proceeds to the next method in the list to continue the authentication process.

This document describes how to configure AAA on the RADIUS server. For details about the configuration on the TACACS+ server, see the *Configuring TACACS+*.

AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

VRF-Enabled AAA Group

Virtual private networks (VPNs) enable users to share bandwidths securely on the backbone networks of Internet service providers (ISPs). A VPN is a site set consisting of shared routes. An STA site connects to the network of an ISP through one or multiple interfaces. AAA supports assigning a VPN routing forwarding (VRF) table to each user-defined server group.

When AAA is implemented by the server in a group assigned with a VRF table, the NAS sends request packets to the remote servers in the server group. The source IP address of request packets is an address selected from the VRF table according to the IP addresses of the remote servers.

If you run the **ip radius/tacacs+ source-interface** command to specify the source interface for the request packets, the IP address obtained from the source interface takes precedence over the source IP address selected from the VRF table.

Overview

Feature	Description
AAA Authentication	Verifies whether users can access the Internet.
AAA Authorization	Determines what services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.
Multi-Domain AAA	Creates domain-specific AAA schemes for 802.1X stations (STAs) in different domains.

2.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. The authentication service verifies whether users can access the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can use only the authentication service of AAA.

To configure AAA authentication, you need to first configure an authentication method list. Applications perform authentication according to the method list. The method list defines the types of authentication and the sequence in which they are performed. Authentication methods are implemented by specified applications. The only exception is the default method list. All applications use the default method list if no method list is configured.

AAA Authentication Scheme

- No authentication (**none**)

The identity of trusted users is not checked. Normally, the no-authentication (None) method is not used.

- Local authentication (**local**)

Authentication is performed on the NAS, which is configured with user information (including usernames, passwords, and AV pairs). Before local authentication is enabled, run the **username password/secret** command to create a local user database.

- Remote server group authentication (**group**)

Authentication is performed jointly by the NAS and a remote server group through RADIUS or TACACS+. A server group consists of one or more servers of the same type. User information is managed centrally on a remote server, thus realizing multi-device centralized and unified authentication with high capacity and reliability. You can configure local authentication as standby to avoid authentication failures when all the servers in the server group fail.

AAA Authentication Types

Ruijie products support the following authentication types:

- Login authentication

Users log in to the command line interface (CLI) of the NAS for authentication through Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).

- Enable authentication

After users log in to the CLI of the NAS, the users must be authenticated before CLI permission update. This process is called Enable authentication (in Privileged EXEC mode).

- Point-to-Point Protocol (PPP) authentication

PPP authentication is performed for users that initiate dial-up access through PPP.

- Dot1X (IEEE802.1X) authentication

Dot1X (IEEE802.1X) authentication is performed for users that initiate dial-up access through IEEE802.1X.

- iPortal (built-in portal) authentication

iPortal authentication is performed by the first generation portal server.

- Web (second generation portal) authentication

Web authentication is performed by the second generation portal server.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authentication Scheme

By default, no AAA authentication scheme is configured.

Before you configure an AAA authentication scheme, determine whether to use local authentication or remote server authentication. If the latter is to be implemented, configure a RADIUS or TACACS+ server in advance. If local authentication is selected, configure the local user database information on the NAS.

Configuring an AAA Authentication Method List

By default, no AAA authentication method list is configured.

Determine the access mode to be configured in advance. Then configure authentication methods according to the access mode.

2.3.2 AAA Authorization

AAA authorization allows administrators to control the services or permissions of users. After AAA authorization is enabled, the NAS configures the sessions of users according to the user configuration files stored on the NAS or servers. After authorization, users can use only the services or have only the permissions permitted by the configuration files.

AAA Authorization Scheme

- Direct authorization (**none**)

Direct authorization is intended for highly trusted users, who are assigned with the default permissions specified by the NAS.

- Local authorization (**local**)

Local authorization is performed on the NAS, which authorizes users according to the AV pairs configured for local users.

- Remote server-group authorization (**group**)

Authorization is performed jointly by the NAS and a remote server group. You can configure local or direct authorization as standby to avoid authorization failures when all the servers in the server group fail.

AAA Authorization Types

- EXEC authorization

After users log in to the CLI of the NAS, the users are assigned with permission levels (0 to 15).

- Config-commands authorization

Users are assigned with the permissions to run specific commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

After users log in through consoles, the users are authorized to run commands.

- Command authorization

Authorize users with commands after login to the CLI of the NAS.

- Network authorization

After users access the Internet, the users are authorized to use the specific session services. For example, after users access the Internet through PPP and Serial Line Internet Protocol (SLIP), the users are authorized to use the data service, bandwidth, and timeout service.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Authorization Scheme

By default, no AAA authorization scheme is configured.

Before you configure an AAA authorization scheme, determine whether to use local authorization or remote server-group authorization. If remote server-group authorization needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local authorization needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Authorization Method List

By default, no AAA authorization method list is configured.

Determine the access mode to be configured in advance. Then configure authorization methods according to the access mode.

2.3.3 AAA Accounting

In AAA, accounting is an independent process of the same level as authentication and authorization. During the accounting process, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server, which records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

In AAA configuration, accounting scheme configuration is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, which collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed jointly by the NAS and a remote server group. You can configure local accounting as standby to avoid accounting failures when all the servers in the server group fail.

AAA Accounting Types

- EXEC accounting

Accounting is performed when users log in to and out of the CLI of the NAS.

- Command accounting

Records are kept on the commands that users run on the CLI of the NAS.

- Network accounting

Records are kept on the sessions that users set up after completing 802.1X and Web authentication to access the Internet.

Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Accounting Scheme

By default, no AAA accounting method is configured.

Before you configure an AAA accounting scheme, determine whether to use local accounting or remote server-group accounting. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. If local accounting needs to be implemented, configure the local user database information on the NAS.

Configuring an AAA Accounting Method List

By default, no AAA accounting method list is configured.

Determine the access mode to be configured in advance. Then configure accounting methods according to the access mode.

2.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide the AAA services to users in different domains. The user AVs (such as usernames and passwords, service types, and permissions) may vary with different domains. It is necessary to configure domains to differentiate the user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

Our products support the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

The fourth format (userid) does not contain a domain name, and it is considered to use the **default** domain name.

The NAS provides the domain-based AAA service based on the following principles:

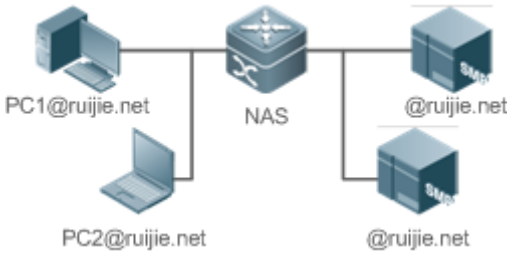
- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.

- Searches for the corresponding AAA method list name according to the domain configuration information on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides the AAA services based on the method list.

If any of the preceding procedures fails, the AAA services cannot be provided.

Figure 2-4 shows the typical multi-domain topology.

Figure 2-4



Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Method List

By default, no AAA method list is configured.

For details, see section 5.2.1, section 5.2.2, and section 5.2.3.

Enabling the Domain-Based AAA Service

By default, the domain-based AAA service is disabled.

To enable the domain-based AAA service, run the **aaa domain enable** command.

Creating a Domain

By default, no domain is configured.

To configure a domain, run the **aaa domain** *domain-name* command.

Configuring an AV Set for a Domain

By default, no domain AV set is configured.

A domain AV set contains the following elements: AAA method lists, the maximum number of online users, whether to remove the domain name from the username, and whether the domain name takes effect.

Displaying Domain Configuration

To display domain configuration, run the **show aaa domain** command.

The system supports a maximum of 32 domains.

2.4 Configuration

Configuration	Description and Command	
Configuring AAA Authentication	Mandatory if user identities need to be verified.	
	aaa new-model	Enables AAA.
	aaa authentication login	Defines a method list of login authentication.
	aaa authentication enable	Defines a method list of Enable authentication.
	aaa authentication dot1x	Defines a method list of 802.1X authentication.
	aaa authentication ppp	Defines a method list of PPP authentication.
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the maximum lockout time after a login failure.
	aaa local user allow public account	Enables local account (**username** or **subs**) sharing in Web and iPortal authentication.
Configuring AAA Authorization	Mandatory if different permissions and services need to be assigned to users.	
	aaa new-model	Enables AAA.
	aaa authorization exec	Defines a method list of EXEC authorization.
	aaa authorization commands	Defines a method list of command authorization.
	aaa authorization network	Configures a method list of network authorization.
	authorization exec	Applies EXEC authorization methods to a specified VTY line.
	authorization commands	Applies command authorization methods to a specified VTY line.
Configuring AAA Accounting	Mandatory if accounting, statistics, and tracking need to be performed on the network resource usage of users.	
	aaa new-model	Enables AAA.
	aaa accounting exec	Defines a method list of EXEC accounting.
	aaa accounting commands	Defines a method list of command accounting.
	aaa accounting network	Defines a method list of network accounting.

Configuration	Description and Command	
	accounting exec	Applies EXEC accounting methods to a specified VTY line.
	accounting commands	Applies command accounting methods to a specified VTY line.
	aaa accounting update	Enables accounting update.
	aaa accounting update periodic	Configures the accounting update interval.
Configuring an AAA Server Group	⚠ Recommended if a server group needs to be configured to handle AAA through different servers in the group.	
	aaa group server	Creates a user-defined AAA server group.
	server	Adds an AAA server group member.
	ip vrf forwarding	Configures the VRF attribute of an AAA server group.
Configuring the Domain-Based AAA Service	⚠ Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.
	aaa domain	Creates a domain and enters domain configuration mode.
	authentication dot1x	Associates the domain with an 802.1X authentication method list.
	accounting network	Associates the domain with a network accounting method list.
	authorization network	Associates the domain with a network authorization method list.
	state	Configures the domain status.
	username-format	Configures whether to contain the domain name in usernames.
	access-limit	Configures the maximum number of domain users.

2.4.1 Configuring AAA Authentication

Configuration Effect

Verify whether users are able to obtain access permission.

Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the configured sequence.

- The next authentication method is executed only when the current method does not respond. If the current method fails, the next method will be not tried.
- When the **none** method is used, users can get access even when no authentication method gets response. Therefore, the **none** method is used only as standby.

Normally, do not use None authentication. You can use the **none** method as the last optional authentication method in special cases. For example, all the users who may request access are trusted users and the users' work must not be delayed by system faults. Then you can use the **none** method to assign access permissions to these users when the authentication server does not respond. It is recommended that the local authentication method be added before the **none** method.

- If AAA authentication is enabled but no authentication method is configured and the default authentication method does not exist, users can directly log in to the Console without being authenticated. If users log in by other means, the users must pass local authentication.
- When a user enters the CLI after passing login authentication (the **none** method is not used), the username is recorded. When the user performs Enable authentication, the user is not prompted to enter the username again, because the username that the user entered during login authentication is automatically filled in. However, the user must enter the password previously used for login authentication.
- The username is not recorded if the user does not perform login authentication when entering the CLI or the **none** method is used during login authentication. Then, a user is required to enter the username each time when performing Enable authentication.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of Login Authentication

- Run the **aaa authentication login** command to configure a method list of login authentication.
- This configuration is mandatory if you need to configure a login authentication method list (including the configuration of the default method list).
- By default, no method list of login authentication is configured.

Defining a Method List of Enable Authentication

- Run the **aaa authentication enable** command to configure a method list of Enable authentication.
- This configuration is mandatory if you need to configure an Enable authentication method list. (You can configure only the default method list.)
- By default, no method list of Enable authentication is configured.

Defining a Method List of 802.1X Authentication

- Run the **aaa authentication dot1x** command to configure a method list of 802.1X authentication.
- This configuration is mandatory if you need to configure an 802.1X authentication method list (including the configuration of the default method list).
- By default, no method list of 802.1X authentication is configured.

Defining a Method List of PPP Authentication

- Run the **aaa authentication ppp** command to configure a method list of PPP authentication.
- This configuration is mandatory if you need to configure an authentication method list for PPP dial-up access.
- By default, no method list of PPP authentication is configured.

Defining a Method List of Web Authentication

- Run the **aaa authentication web-auth** command to configure a method list of Web authentication.
- This configuration is mandatory if you need to configure a Web authentication method list (including the configuration of the default method list).
- By default, no method list of Web authentication is configured.

Defining a Method List of iPortal Web Authentication

- Run the **aaa authentication iportal** command to configure a method list of iPortal Web authentication.
- This configuration is mandatory if you need to configure an iPortal Web authentication method list (including the configuration of the default method list).
- By default, no method list of iPortal Web authentication is configured.

Defining a General Method List of 802.1X, Web, and iPortal Web Authentication

- Run the **aaa authentication general** command to configure a general method list of 802.1X, Web, and iPortal Web authentication.
- If the **aaa authentication dot1x/web-auth/iportal** commands are run, their corresponding effects previal.
- By default, no general method list is configured.

Defining a Method List of SSL VPN Authentication

- Run the **aaa authentication sslvpn** command to configure a method list of SSL VPN authentication.
- This configuration is mandatory if you need to configure an SSL VPN authentication method list (including the configuration of the default method list).
- By default, no method list of SSL VPN authentication is configured.

Setting the Maximum Number of Login Attempts

- Optional.

- By default, a user is allowed to enter passwords up to three times during login.

Setting the Maximum Lockout Time After a Login Failure

- Optional.
- By default, a user is locked for 15 minutes after entering wrong passwords three times.

Enabling Local Account (username or subs) Sharing in Web and iPortal Authentication

- (Optional) This configuration is supported only on EG products. This function is supported by default on other types of Ruijie products.
- By default, a local account cannot be shared among multiple STAs.

Verification

- Run the **show aaa method-list** command to display the configured method lists.
- Run the **show aaa lockout** command to display the settings of the maximum number of login attempts and the maximum lockout time after a login failure.
- Run the **show running-config** command to display the authentication method lists associated with login authentication and 802.1X authentication.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a login authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported. **subs**: Indicates that the subs database is used for authentication.

Command Mode	Global configuration mode
Usage Guide	In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of Enable Authentication

Command	**aaa authentication enable default** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an Enable authentication method list in characters. *method*: Indicates authentication methods from **enable**, **local**, **none**, and **group**. A method list contains up to four methods. **enable**: Indicates that the password that is configured using the **enable** command is used for authentication. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of 802.1X Authentication

Command	**aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an 802.1X authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	If the AAA 802.1X authentication service is enabled on the NAS, users must perform 802.1X authentication negotiation through AAA. Run the **aaa authentication dot1x** command to configure the default or optional method lists for 802.1X authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a Method List of PPP, Web, iPortal or SSL VPN Authentication

Command	**aaa authentication** { **ppp | web-auth** | **iportal** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]

Parameter Description	**ppp:** Configures a method list of PPP authentication. **web-auth**: Configures a method list of Web authentication. **iportal**: Configures a method list of iportal authentication. **sslvpn**: Configures a method list of SSL VPN authentication. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a PPP authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported. **subs**: Specifies the SUBS authentication method using the SUBS database.
Command Mode	Global configuration mode
Usage Guide	If the AAA PPP authentication service is enabled on the NAS, users must perform PPP authentication negotiation through AAA. Run the **aaa authentication ppp** command to configure the default or optional method lists for PPP authentication. In a method list, the next method is executed only when the current method does not receive response.

Defining a General Method List of 802.1X, Web, and iPortal Web Authentication

Command	**aaa authentication general** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted for 802.1X, Web and iPortal Web authentication. *list-name*: Indicates the name of a general authentication method list in characters. *method*: Indicates authentication methods from **local**, **none**, **group**, and **subs**. A method list contains up to four methods. **local**: Indicates that the local user database is used for authentication. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for authentication. Currently, the RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum number of times a user can attempt to login.

Setting the Maximum Number of Login Attempts

Command	**aaa local authentication attempts** *max-attempts*
Parameter Description	*max-attempts*: Indicates the maximum number of login attempts. The value ranges from 1 to 2,147,483,647.
Command Mode	Global configuration mode

Usage Guide	Use this command to set the maximum number of times a user can attempt to login.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time*: Indicates the time during which a user is locked after entering wrong passwords up to the specified times. The value ranges from 1 to 43200, in the unit of minutes.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum time during which a user is locked after entering wrong passwords up to the specified times.

Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local user allow public account**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to configure local account (**username** or **subs**) sharing among multiple STAs in Web authentication or iPortal Web authentication.

Configuration Example

Configuring AAA Login Authentication

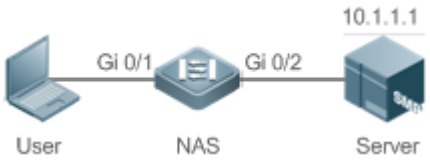
Configure a login authentication method list on the NAS containing **group** *radius* and **local** methods in order.

Scenario Figure 2-5	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Step 3: Configure an AAA authentication method list for login authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the configured method list to an interface or line. Skip this step if the default authentication method is used.
NAS	`Ruijie#configure terminal` `Ruijie(config)#username user password  pass` `Ruijie(config)#aaa new-model`

	Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key ruijie Ruijie(config)#aaa authentication login list1 group radius local Ruijie(config)#line vty 0 20 Ruijie(config-line)#login authentication list1 Ruijie(config-line)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication login list1 group radius local Accounting method-list: Authorization method-list:
	Assume that a user remotely logs in to the NAS through Telnet. The user is prompted to enter the username and password on the CLI. The user must enter the correct username and password to access the NAS.
User	User Access Verification Username:user Password:pass

Configuring AAA Enable Authentication

Configure an Enable authentication method list on the NAS containing **group** *radius*, **local**, and then **enable** methods in order.

Scenario **Figure 2-6**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be

	implemented. Configure Enable authentication passwords on the NAS if you use Enable password authentication. Step 3: Configure an AAA authentication method list for Enable authentication users. You can define only one Enable authentication method list globally. You do not need to define the list name but just default it. After that, it will be applied automatically.
NAS	`Ruijie#configure terminal` `Ruijie(config)#username user privilege 15 password  pass` `Ruijie(config)#enable secret w` `Ruijie(config)#aaa new-model` `Ruijie(config)#radius-server host 10.1.1.1` `Ruijie(config)#radius-server key ruijie` `Ruijie(config)#aaa authentication enable default group radius local enable`
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	`Ruijie#show aaa method-list` `Authentication method-list:` `aaa authentication enable default group radius local enable` `Accounting method-list:` `Authorization method-list:`
	The CLI displays an authentication prompt when the user level is updated to level 15. The user must enter the correct username and password to access the NAS.
NAS	`Ruijie>enable` `Username:user` `Password:pass` `Ruijie#`

Configuring AAA 802.1X Authentication

Configure an 802.1X authentication method list on the NAS containing **group** *radius*, and then **local** methods in order.

Scenario **Figure 2-7**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS server in advance if group-server authentication needs to be implemented. Configure the local user database information on the NAS if local authentication needs to be implemented. (This example requires the configuration of a RADIUS server and local database information.) Currently, 802.1X authentication does not support TACACS+. Step 3: Configure an AAA authentication method list for 802.1X authentication users. (This example uses **group** *radius* and **local** in order.) Step 4: Apply the AAA authentication method list. Skip this step if the default authentication method is used. Step 5: Enable 802.1X authentication on an interface.
NAS	`Ruijie#configure terminal` `Ruijie(config)#username user1 password  pass1` `Ruijie(config)#username user2 password  pass2` `Ruijie(config)#aaa new-model` `Ruijie(config)#radius-server host 10.1.1.1` `Ruijie(config)#radius-server key ruijie` `Ruijie(config)#aaa authentication dot1x default group radius local` `Ruijie(config)#interface gigabitEthernet 0/1` `Ruijie(config-if-gigabitEthernet 0/1)#dot1 port-control auto` `Ruijie(config-if-gigabitEthernet 0/1)#exit`
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	`Ruijie#show aaa method-list` `Authentication method-list:` `aaa authentication dot1x default group radius local` `Accounting method-list:` `Authorization method-list:`

Common Errors

- No RADIUS server or TACACS+ server is configured.
- Usernames and passwords are not configured in the local database.

2.4.2 Configuring AAA Authorization

Configuration Effect

- Determine what services or permissions authenticated users can enjoy.

Notes

- EXEC authorization is often used with login authentication, which can be implemented on the same line. Authorization and authentication can be performed using different methods and servers. Therefore, the results of the same user may be different. If a user passes login authentication but fails in EXEC authorization, the user cannot enter the CLI.
- The authorization methods in an authorization scheme are executed in accordance with the method configuration sequence. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: The RGOS can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Authorization

- Run the **aaa authorization exec** command to configure a method list of EXEC authorization.
- This configuration is mandatory if you need to configure an EXEC authorization method list (including the configuration of the default method list).
- By default, no EXEC authorization method list is configured.

The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)

Defining a Method List of Command Authorization

- Run the **aaa authorization commands** command to configure a method list of command authorization.
- This configuration is mandatory if you need to configure a command authorization method list (including the configuration of the default method list).
- By default, no command authorization method list is configured.

Configuring a Method List of Network Authorization

- Run the **aaa authorization network** command to configure a method list of network authorization.
- This configuration is mandatory if you need to configure a network authorization method list (including the configuration of the default method list).
- By default, no authorization method is configured.

Applying EXEC Authorization Methods to a Specified VTY Line

- Run the **authorization exec** command in line configuration mode to apply EXEC authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Applying Command Authorization Methods to a Specified VTY Line

- Run the **authorization commands** command in line configuration mode to apply command authorization methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command authorization method list to a specified VTY line.
- By default, all VTY lines are associated with the default authorization method list.

Enabling Authorization for Commands in Configuration Modes

- Run the **aaa authorization config-commands** command to enable authorization for commands in configuration modes.
- By default, authorization is disabled for commands in configuration modes.

Enabling Authorization for the Console to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for the Console to run commands.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Authorization

Command	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC authorization method list in characters. *method*: Specifies authentication methods from **local**, **none**, and **group**. A method list contains up to four methods. **local**: Indicates that the local user database is used for EXEC authorization. **none**: Indicates that EXEC authorization is not performed. **group**: Indicates that a server group is used for EXEC authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS supports authorization of the users who log in to the CLI of the NAS to assign the users CLI operation permission levels (0 to 15). Currently, EXEC authorization is performed only on the users who have passed login authentication. If a user fails in EXEC authorization, the user cannot enter the CLI. After you configure EXEC authorization methods, apply the methods to the VTY lines that require EXEC authorization; otherwise, the methods will not take effect.

Defining a Method List of Command Authorization

Command	**aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command authorization is not performed. **group**: Indicates that a server group is used for command authorization. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS supports authorization of the commands executable by users. When a user enters a command, AAA sends the command to the authentication server. If the authentication server permits the execution, the command is executed. If the authentication server forbids the execution, the command is not executed and a message is displayed showing that the execution is rejected.

	When you configure command authorization, specify the command level, which is used as the default level. (For example, if a command above Level 14 is visible to users, the default level of the command is 14.) After you configure command authorization methods, apply the methods to the VTY lines that require command authorization; otherwise, the methods will not take effect.

Configuring a Method List of Network Authorization

Command	**aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network authorization method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that authentication is not performed. **group**: Indicates that a server group is used for network authorization. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS supports authorization of network-related service requests such as PPP and SLIP requests. After authorization is configured, all authenticated users or interfaces are authorized automatically. You can configure three different authorization methods. The next authorization method is executed only when the current method does not receive response. If authorization fails using a method, the next method will be not tried. RADIUS or TACACS+ servers return a series of AV pairs to authorize authenticated users. Network authorization is based on authentication. Only authenticated users can perform network authorization.

Enabling Authorization for Commands in Configuration Modes (Including the Global Configuration Mode and Sub-Modes)

Command	**aaa authorization config-commands**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If you need to enable authorization for commands only in non-configuration modes (for example, privileged EXEC mode), disable authorization in configuration modes by using the **no** form of this command. Then users can run commands in configuration mode and sub-modes without authorization.

Enabling Authorization for the Console to Run Commands

Command	**aaa authorization console**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	The RGOS can differentiate between the users who log in through the Console and the users who log in through other types of clients. You can enable or disable command authorization for the users who log in through the Console. If command authorization is disabled for these users, the command authorization method list applied to the Console line no longer takes effect.

Configuration Example

Configuring AAA EXEC Authorization

Configure login authentication and EXEC authorization for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC authorization is performed on a RADIUS server. If the RADIUS server does not respond, users are redirected to the local authorization.

Scenario **Figure 2-8**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used. EXEC authorization is often used with login authentication, which can be implemented on the same line.
NAS	`Ruijie#configure terminal` `Ruijie(config)#username user password  pass` `Ruijie(config)#username user privilege 6` `Ruijie(config)#aaa new-model` `Ruijie(config)#radius-server host 10.1.1.1` `Ruijie(config)#radius-server key  test` `Ruijie(config)#aaa authentication login list1 group local` `Ruijie(config)#aaa authorization exec list2 group radius local` `Ruijie(config)#line vty 0 4` `Ruijie(config-line)#login authentication list1` `Ruijie(config-line)# authorization exec list2` `Ruijie(config-line)#exit`

Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: Authorization method-list: aaa authorization exec list2 group radius local
	Ruijie# show running-config aaa new-model ! aaa authorization exec list2 group local aaa authentication login list1 group radius local ! username user password pass username user privilege 6 ! radius-server host 10.1.1.1 radius-server key 7 093b100133 ! line con 0 line vty 0 4 authorization exec list2 login authentication list1 ! End

Configuring AAA Command Authorization

Provide command authorization for login users according to the following default authorization method: Authorize level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

Scenario **Figure 2-9**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types. Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Ruijie#configure terminal Ruijie(config)#username user1 password pass1 Ruijie(config)#username user1 privilege 15 Ruijie(config)#aaa new-model Ruijie(config)#tacacs-server host 192.168.217.10 Ruijie(config)#tacacs-server key aaa Ruijie(config)#aaa authentication login default local Ruijie(config)#aaa authorization commands 15 default group tacacs+ local Ruijie(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: Authorization method-list: aaa authorization commands 15 default group tacacs+ local
	Ruijie#show run ! aaa new-model

```
!
aaa authorization console
aaa authorization commands 15 default group tacacs+ local
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

Configuring AAA Network Authorization

Scenario **Figure 2-10**	
Configuration Steps	Step 1: Enable AAA. Step 2: Configure a RADIUS or TACACS+ server in advance if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure the local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types.

	Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Ruijie#configure terminal Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authorization network default group radius none Ruijie(config)# end
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: Accounting method-list: Authorization method-list: aaa authorization network default group radius none

Common Errors

N/A

2.4.3 Configuring AAA Accounting

Configuration Effect

- Record the network resource usage of users.
- Record the user login and logout processes and the commands executed by users during device management.

Notes

About accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the method configuration sequence. The next accounting method is executed only when the current method does not receive response. If accounting fails using a method, the next method will be not tried.
- After the default accounting method list is configured, it is applied to all VTY lines automatically. If a non-default accounting method list is applied to a line, it will replace the default one. If you apply an undefined method list to a line,

the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start accounting is not performed for a user upon login, Stop accounting will not be performed when the user logs out.

Command accounting

- Only the TACACS+ protocol supports command accounting.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Accounting

- Run the **aaa accounting exec** command to configure a method list of EXEC accounting.
- This configuration is mandatory if you need to configure an EXEC accounting method list (including the configuration of the default method list).
- The default access permission level of EXEC users is the lowest. (Console users can connect to the NAS through the Console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user and SSH user.)
- By default, no EXEC accounting method list is configured.

Defining a Method List of Command Accounting

- Run the **aaa accounting commands** command to configure a method list of command accounting.
- This configuration is mandatory if you need to configure a command accounting method list (including the configuration of the default method list).
- By default, no command accounting method list is configured. Only the TACACS+ protocol supports command accounting.

Defining a Method List of Network Accounting

- Run the **aaa accounting network** command to configure a method list of network accounting.
- This configuration is mandatory if you need to configure a network accounting method list (including the configuration of the default method list).
- By default, no network accounting method list is configured.

Applying EXEC Accounting Methods to a Specified VTY Line

- Run the **accounting exec** command in line configuration mode to apply EXEC accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply an EXEC accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying Command Accounting Methods to a Specified VTY Line

- Run the **accounting commands** command in line configuration mode to apply command accounting methods to a specified VTY line.
- This configuration is mandatory if you need to apply a command accounting method list to a specified VTY line.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Applying 802.1X Network Accounting Methods

- Run the **dot1x accounting network** command to configure 802.1X network accounting methods.
- This configuration is mandatory if you need to specify 802.1X network accounting methods.
- You do not need to run this command if you apply the default method list.
- By default, all VTY lines are associated with the default accounting method list.

Enabling Accounting Update

- Optional.
- It is recommended that accounting update be configured for improved accounting accuracy.
- By default, accounting update is disabled.

Configuring the Accounting Update Interval

- Optional.
- It is recommended that the accounting update interval not be configured unless otherwise specified.

Verification

Run the **show running-config** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command	Global configuration mode

Mode	
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of an EXEC accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that EXEC accounting is not performed. **group**: Indicates that a server group is used for EXEC accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS enables EXEC accounting only when login authentication is completed. EXEC accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, when a user logs in to the CLI of the NAS, the NAS sends a start-accounting message to the authentication server. When the user logs out, the NAS sends a stop-accounting message to the authentication server. If the NAS does not send a start-accounting message when the user logs in, the NAS will not send a stop-accounting message when the user logs out. After you configure EXEC accounting methods, apply the methods to the VTY lines that require EXEC accounting; otherwise, the methods will not take effect.

Defining a Method List of Command Accounting

Command	**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*level*: Indicates the command level for which accounting will be performed. The value ranges from 0 to 15. After a command of the configured level is executed, the accounting server records related information based on the received accounting packet. **default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a command accounting method list in characters. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that command accounting is not performed. **group**: Indicates that a server group is used for command accounting. Currently, the TACACS+ server group is supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS enables command accounting only when login authentication is completed. Command accounting is not performed if login authentication is not performed or the **none** authentication method is used. After accounting is enabled, the NAS records information about the commands of the configured level that users run and sends the information to the authentication server. After you configure command accounting methods, apply the methods to the VTY lines that require

	command accounting; otherwise, the methods will not take effect.

Defining a Method List of Network Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: With this parameter used, the configured method list will be defaulted. *list-name*: Indicates the name of a network accounting method list in characters. **start-stop**: Indicates that a start-accounting message and a stop-accounting message are sent when a user accesses a network and when the user disconnects from the network respectively. The start-accounting message indicates that the user is allowed to access the network, regardless of whether accounting is successfully enabled. *method*: Indicates authentication methods from **none** and **group**. A method list contains up to four methods. **none**: Indicates that network accounting is not performed. **group**: Indicates that a server group is used for network accounting. Currently, the RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	The RGOS sends record attributes to the authentication server to perform accounting of user activities. The **start-stop** keyword is used to configure user accounting options.

Enabling Accounting Update

Command	**aaa accounting update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to enable accounting update.

Configuring the Accounting Update Interval

Command	**aaa accounting update periodic** *interval*
Parameter Description	*Interval*: Indicates the accounting update interval, in the unit of minutes. The shortest is 1 minute.
Command Mode	Global configuration mode
Usage Guide	Accounting update cannot be used if the AAA services are not enabled. After the AAA services are enabled, run this command to configure the accounting update interval.

Configuration Example

Configuring AAA EXEC Accounting

Configure login authentication and EXEC accounting for users on VTY lines 0 to 4. Login authentication is performed in local mode, and EXEC accounting is performed on a RADIUS server.

Scenario **Figure 2-11**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	Ruijie#configure terminal Ruijie(config)#username user password pass Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authentication login list1 group local Ruijie(config)#aaa accounting exec list3 start-stop group radius Ruijie(config)#line vty 0 4 Ruijie(config-line)#login authentication list1 Ruijie(config-line)# accounting exec list3 Ruijie(config-line)#exit
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication login list1 group local Accounting method-list: aaa accounting exec list3 start-stop group radius Authorization method-list:

```
Ruijie# show running-config
aaa new-model
!
aaa accounting exec list3 start-stop group radius
aaa authentication login list1 group local
!
username user password  pass
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting  exec list3
 login authentication list1
!
End
```

Configuring AAA Command Accounting

Configure command accounting for login users according to the default accounting method. Login authentication is performed in local mode, and command accounting is performed on a TACACS+ server.

Scenario **Figure 2-12**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	`Ruijie#configure terminal`

	Ruijie(config)#username user1 password pass1 Ruijie(config)#username user1 privilege 15 Ruijie(config)#aaa new-model Ruijie(config)#tacacs-server host 192.168.217.10 Ruijie(config)#tacacs-server key aaa Ruijie(config)#aaa authentication login default local Ruijie(config)#aaa accounting commands 15 default start-stop group tacacs+
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+ Authorization method-list:
	Ruijie#show run ! aaa new-model ! aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local ! ! nfpp ! vlan 1 !

	username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 ! ! end

Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X STAs, and configure a RADIUS remote server for authentication and accounting.

Scenario **Figure 2-13**	
Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, configure a RADIUS server in advance. Step 3: Configure an AAA accounting method list according to different access modes and service types. Step 4: Apply the configured AAA accounting method list. Skip this step if the default accounting method is used. Accounting is performed only when 802.1X authentication is completed.
NAS	Ruijie#configure terminal Ruijie(config)#username user password pass Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 10.1.1.1 Ruijie(config)#radius-server key test Ruijie(config)#aaa authentication dot1x aut1x group radius local

	Ruijie(config)#aaa accounting network acc1x start-stop group radius Ruijie(config)#dot1x authentication aut1x Ruijie(config)#dot1x accounting acc1x Ruijie(config)#interface gigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#dot1 port-control auto Ruijie(config-if-GigabitEthernet 0/1)#exit
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Ruijie#show aaa method-list Authentication method-list: aaa authentication dot1x aut1x group radius local Accounting method-list: aaa accounting network acc1x start-stop group radius Authorization method-list:

Common Errors

N/A

2.4.4 Configuring an AAA Server Group

Configuration Effect

- Create a user-defined server group and add one or more servers to the group.
- When you configure authentication, authorization, and accounting method lists, name the methods after the server group name so that the servers in the group are used to handle authentication, authorization, and accounting requests.
- Use self-defined server groups to separate authentication, authorization, and accounting.

Notes

In a user-defined server group, you can specify and apply only the servers in the default server group.

Configuration Steps

↘ Creating a User-Defined AAA Server Group

- Mandatory.
- Assign a meaningful name to the user-defined server group. Do not use the predefined **radius** and **tacacs+** keywords in naming.

Adding an AAA Server Group Member

- Mandatory.
- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

Configuring the VRF Attribute of an AAA Server Group

- Optional.
- Run the **ip vrf forwarding** command to configure the VRF attribute of an AAA server group.
- By default, the AAA server group belongs to the global VRF table.

Verification

Run the **show aaa group** command to verify the configuration.

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server** {**radius** | **tacacs+**} *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The name must not contain the **radius** and **tacacs+** keywords because they are the names of the default RADIUS and TACACS+ server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. Currently, the RADIUS and TACACS+ server groups are supported.

Adding an AAA Server Group Member

Command	**server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-addr*: Indicates the IP address of a server. *port1*: Indicates the authentication port of a server. (This parameter is supported only by the RADIUS server group.) *port2*: Indicates the accounting port of a server. (This parameter is supported only by the RADIUS server group.)
Command Mode	Server group configuration mode
Usage Guide	When you add servers to a server group, the default ports are used if you do not specify ports.

Configuring the VRF Attribute of an AAA Server Group

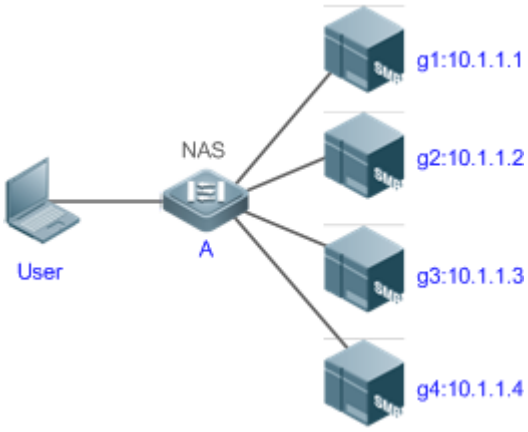
Command	**ip vrf forwarding** *vrf_name*
Parameter Description	*vrf_name*: Indicates the name of a VRF table.

Command Mode	Server group configuration mode
Usage Guide	Use this command to assign a VRF table to the specified server group.

Configuration Example

↘ Creating an AAA Server Group

Create RADIUS server groups named g1 and g2. The IP addresses of the servers in g1 are 10.1.1.1 and 10.1.1.2, and the IP addresses of the servers in g2 are 10.1.1.3 and 10.1.1.4.

Scenario **Figure 2-14**	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable. 2. Enable AAA.
Configuration Steps	Step 1: Configure a server (which belongs to the default server group). Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.
NAS	`Ruijie#configure terminal` `Ruijie(config)#radius-server host 10.1.1.1` `Ruijie(config)#radius-server host 10.1.1.2` `Ruijie(config)#radius-server host 10.1.1.3` `Ruijie(config)#radius-server host 10.1.1.4` `Ruijie(config)#radius-server key secret` `Ruijie(config)#aaa group server radius g1` `Ruijie(config-gs-radius)#server 10.1.1.1` `Ruijie(config-gs-radius)#server 10.1.1.2`

	Ruijie(config-gs-radius)#exit Ruijie(config)#aaa group server radius g2 Ruijie(config-gs-radius)#server 10.1.1.3 Ruijie(config-gs-radius)#server 10.1.1.4 Ruijie(config-gs-radius)#exit
Verification	Run the **show aaa group** and **show run** commands on the NAS to display the configuration.
NAS	Ruijie#show aaa group Type Reference Name ---------- ---------- ---------- radius 1 radius tacacs+ 1 tacacs+ radius 1 g1 radius 1 g2
	Ruijie#show run ! radius-server host 10.1.1.1 radius-server host 10.1.1.2 radius-server host 10.1.1.3 radius-server host 10.1.1.4 radius-server key secret ! aaa group server radius g1 server 10.1.1.1 server 10.1.1.2 ! aaa group server radius g2 server 10.1.1.3 server 10.1.1.4 ! !

Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.
- Only the RADIUS server group can be configured with the VRF attribute.

2.4.5 Configuring the Domain-Based AAA Service

Configuration Effect

Create AAA schemes for 802.1X users in different domains.

Notes

About referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be defined in advance. If the method lists are not defined in advance, when you select them in domain configuration mode, the system prompts that the configurations do not exist.
- The names of the AAA method lists selected in domain configuration mode must be consistent with those of the method lists defined for the AAA service. If they are inconsistent, the AAA service cannot be properly provided to the users in the domain.

About the default domain:

- Default domain: After the domain-based AAA service is enabled, if a username does not carry domain information, the AAA service is provided to the user based on the default domain. If the domain information carried by the username is not configured in the system, the system determines that the user is unauthorized and will not provide the AAA service to the user. If the default domain is not configured initially, it must be created manually.
- When the domain-based AAA service is enabled, the default domain is not configured by default and needs to be created manually. The default domain name is **default**. It is used to provide the AAA service to the users whose usernames do not carry domain information. If the default domain is not configured, the AAA service is not available for the users whose usernames do not carry domain information.

About domain names:

- The domain names carried by usernames and those configured on the NAS are matched in the longest matching principle. For example, if two domains, **domain.com** and **domain.com.cn** are configured on a NAS and a user sends a request carrying **aaa@domain.com**, the NAS determines that the user belongs to **domain.com**, instead of **domain.com.cn**.
- If the username of an authenticated user carries domain information but the domain is not configured on the NAS, the AAA service is not provided to the user.

Configuration Steps

↘ Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Enabling the Domain-Based AAA Service

- Mandatory.
- Run the **aaa domain enable** command to enable the domain-based AAA service.
- By default, the domain-based AAA service is disabled.

Creating a Domain and Entering Domain Configuration Mode

- Mandatory.
- Run the **aaa domain** command to create a domain or enter the configured domain.
- By default, no domain is configured.

Associating the Domain with an 802.1X Authentication Method List

- Run the **authentication dot1x** command to associate the domain with an 802.1X authentication method list.
- This configuration is mandatory if you need to apply a specified 802.1X authentication method list to the domain.
- Currently, the domain-based AAA service is applicable only to 802.1X access.

Associating the Domain with a Network Accounting Method List

- Run the **accounting network** command to associate the domain with a network accounting method.
- This configuration is mandatory if you need to apply a specified network accounting method list to the domain.
- If a domain is not associated with a network accounting method list, by default, the global default method list is used for accounting.

Associating the Domain with a Network Authorization Method List

- Run the **authorization network** command to associate the domain with a network authorization method list.
- This configuration is mandatory if you need to apply a specified network authorization method list to the domain.
- If a domain is not associated with a network authorization method list, by default, the global default method list is used for authorization.

Configuring the Domain Status

- Optional.
- When a domain is in Block state, the users in the domain cannot log in.
- By default, after a domain is created, its state is Active, indicating that all the users in the domain are allowed to request network services.

Configuring Whether to Contain the Domain Name in Usernames

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

Configuring the Maximum Number of Domain Users

- Optional.
- By default, the maximum number of access users allowed in a domain is not limited.

Verification

Run the **show aaa domain** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA services, run this command. None of the rest of AAA commands can be effective if AAA is not enabled.

Enabling the Domain-Based AAA Service

Command	**aaa domain enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the domain-based AAA service.

Creating a Domain and Entering Domain Configuration Mode

Command	**aaa domain** { **default** | *domain-name* }
Parameter Description	**default**: Uses this parameter to configure the default domain. *domain-name*: Indicates the name of the domain to be created.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a domain to provide the domain-based AAA service. The **default** parameter specifies the default domain. If a username does not carry domain information, the NAS uses the method list associated with the default domain to provide the AAA service to the user. The *domain-name* parameter specifies the name of the domain to be created. If the domain name carried by a username matches the configured domain name, the NAS uses the method list associated with this domain to provide the AAA

	service to the user. The system supports a maximum of 32 domains.

Associating the Domain with an 802.1X Authentication Method List

Command	**authentication dot1x** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a 802.1X authentication method list.

Associating the Domain with a Network Accounting Method List

Command	**accounting network** { **default |** *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a network accounting method list.

Associating the Domain with a Network Authorization Method List

Command	**authorization network** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	

Configuring the Domain Status

Command	**state** { **block** | **active** }
Parameter Description	**block**: Indicates that the configured domain is invalid. **active**: Indicates that the configured domain is valid.
Command Mode	Domain configuration mode
Usage Guide	Use this command to make the configured domain valid or invalid.

Configuring Whether to Contain the Domain Name in Usernames

Command	**username-format** { **without-domain** | **with-domain** }
Parameter Description	**without-domain**: Indicates to remove domain information from usernames. **with-domain**: Indicates to keep domain information in usernames.
Command Mode	Domain configuration mode

Usage Guide	Use this command in domain configuration mode to determine whether to include domain information in usernames when the NAS interacts with authentication servers in a specified domain.

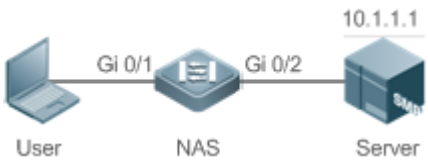
Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain. This limit is applicable only to 802.1X STAs.
Command Mode	Domain configuration mode
Usage Guide	Use this command to limit the number of access users in a domain.

Configuration Example

Configuring the Domain-Based AAA Services

Configure authentication and accounting through a RADIUS server to 802.1X users (username: *user*@domain.com) that access the NAS. The usernames that the NAS sends to the RADIUS server do not carry domain information, and the number of access users is not limited.

Scenario Figure 2-15	
Configuration Steps	The following example shows how to configure RADIUS authentication and accounting, which requires the configuration of a RADIUS server in advance. Step 1: Enable AAA. Step 2: Define an AAA method list. Step 3: Enable the domain-based AAA service. Step 4: Create a domain. Step 5: Associate the domain with the AAA method list. Step 6: Configure the domain attribute.
NAS	`Ruijie#configure terminal` `Ruijie(config)#aaa new-model` `Ruijie(config)#radius-server host 10.1.1.1` `Ruijie(config)#radius-server key  test` `Ruijie(config)#aaa authentication dot1x default group radius` `Ruijie(config)#aaa accounting network list3 start-stop group radius` `Ruijie(config)# aaa domain enable` `Ruijie(config)# aaa domain domain.com`

	Ruijie(config-aaa-domain)# authentication dot1x default Ruijie(config-aaa-domain)# accounting network list3 Ruijie(config-aaa-domain)# username-format without-domain
Verification	Run the **show run** and **show aaa domain** command on the NAS to display the configuration.
NAS	Ruijie#show aaa domain domain.com =============Domain domain.com============= State: Active Username format: With-domain Access limit: No limit 802.1X Access statistic: 0 Selected method list: authentication dot1x default accounting network list3
	Ruijie#show run Building configuration... Current configuration : 1449 bytes version RGOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67) co-operate enable ! aaa new-model aaa domain enable ! aaa domain domain.com authentication dot1x default accounting network list3 ! aaa accounting network list3 start-stop group radius

	aaa authentication dot1x default group radius ! nfpp ! no service password-encryption ! radius-server host 10.1.1.1 radius-server key test ! line con 0 line vty 0 4 ! end

Common Errors

N/A

2.4.6 Detecting AAA Heartbeats

Configuration Effect

After this feature is configured, AAA processes and the AAA database send heartbeats to detect whether the peer ends are available.

Notes

Heartbeats are supported on some front-end AAA modules, such as RADIUS and DOT1X modules.

Configuration Steps

↘ Detecting AAA Heartbeats

- Optional.
- By default, this feature is enabled.

Verification

Run the **show run** command to verify the configuration.

Related Commands

↘ Allowing Users to Get Online After Accounting Fails to Start

Command	[no] aaa heartbeat enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Detecting AAA Heartbeats

Scenario Figure 2-16	
Configuration Steps	The following example disables AAA heartbeats.
NAS	Ruijie#configure terminal Ruijie(config)#no aaa heartbeat enable
Verification	Run the **show run** command on the NAS to display the configuration.
NAS	Ruijie#sh run | inc heart
	no aaa heartbeat enable

Common Errors

N/A

2.5 Monitoring

Clearing

Description	Command
Clears the locked users.	**clear aaa local user lockout** {**all** | **user-name** *username* }

Displaying

Description	Command
Displays the accounting update information.	**show aaa accounting update**
Displays the current domain configuration.	**show aaa domain**

Displays the current lockout configuration.	**show aaa lockout**
Displays the AAA server groups.	**show aaa group**
Displays the AAA method lists.	**show aaa method-list**
Displays the AAA users.	**show aaa user**

3 Configuring RADIUS

3.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS works with the Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network, to prevent unauthorized access. In RGOS implementation, a RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the central RADIOUS server, where all user identity authentication information and network service information are stored. In addition to the authentication service, the RADIUS server provides authorization and accounting services for access users.

RADIUS is often applied in network environments that have high security requirements and allow the access of remote users. RADIUS is a completely open protocol and the RADIUS server is installed on many operating systems as a component, for example, on UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server currently.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in the IETF RFC3576. This protocol defines a user offline management method. Devices communicate with the RADIUS server through the Disconnect-Messages (DMs) to bring authenticated users offline. This protocol implements compatibility between devices of different vendors and the RADIUS server in terms of user offline processing.

In the DM mechanism, the RADIUS server actively initiates a user offline request to a device, the device locates a user according to the user session information, user name, and other information carried in the request and brings the user offline. Then, the device returns a response packet that carries the processing result to the RADIUS server, thereby implementing user offline management of the RADIUS server.

Protocols and Standards

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

3.2 Applications

Application	Description
Providing Authentication, Authorization, and Accounting	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.

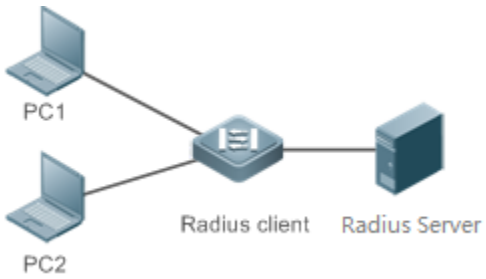
Application	Description
Services for Access Users	
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

3.2.1 Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

RADIUS is typically applied in the authentication, authorization, and accounting of access users. A network device serves as a RADIUS client and transmits user information to a RADIUS server. After completing processing, the RADIUS server returns the authentication acceptance/authentication rejection/accounting response information to the RADIUS client. The RADIUS client performs processing on the access user according to the response from the RADIUS server.

Figure 3-1 Typical RADIUS Networking Topology



Remarks	PC 1 and PC 2 are connected to the RADIUS client as access users in wired or wireless mode, and initiate authentication and accounting requests. The RADIUS client is usually an access switch or aggregate switch. The RADIUS server can be a component built in the Windows 2000/2003, Server (IAS), or UNIX operating system or dedicated server software provided by vendors.

Deployment

- Configure access device information on the RADIUS server, including the IP address and shared key of the access devices.
- Configure the AAA method list on the RADIUS client.
- Configure the RADIUS server information on the RADIUS client, including the IP address and shared key.
- Enable access control on the access port of the RADIUS client.
- Configure the network so that the RADIUS client communicates with the RADIUS server successfully.

3.2.2 Forcing Users to Go Offline

Scenario

The RADIUS server forces authenticated online users to go offline for the sake of management.

See Figure 3-1 for the networking topology.

Deployment

- Add the following deployment on the basis of 3.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

3.3 Features

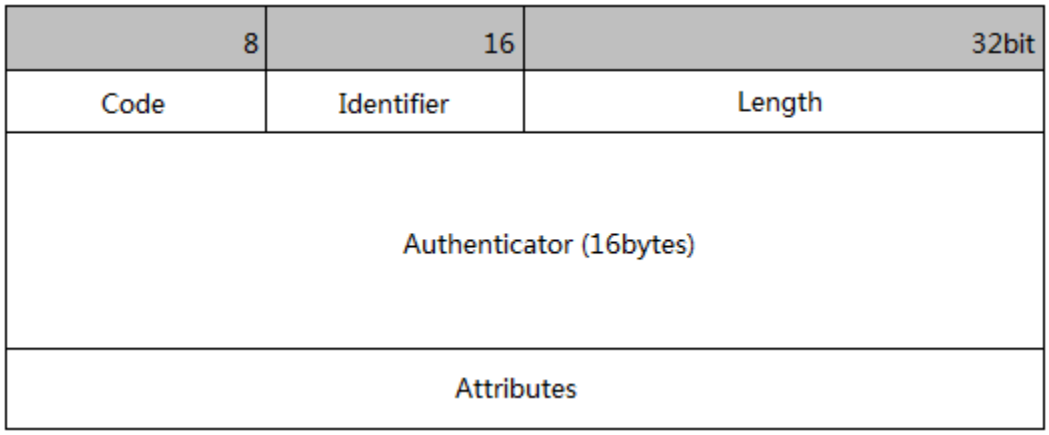
Basic Concepts

Client/Server Mode

- Client: A RADIUS client initiates RADIUS requests and usually runs on a device or NAS. It transmits user information to the RADIUS server, receives responses from the RADIUS server, and performs processing accordingly. The processing includes accepting user access, rejecting user access, or collecting more user information for the RADIUS server.
- Server: Multiple RADIUS clients map to one RADIUS server. The RADIUS server maintains the IP addresses and shared keys of all RADIUS clients as well as information on all authenticated users. It receives requests from a RADIUS client, conducts authentication, authorization, and accounting, and returns processing information to the RADIUS client.

Structure of RADIUS Packets

The following figure shows the structure of RADIUS packets.



- Code: Identifies the type of RADIUS packets, which occupies one byte. The following table lists the values and meanings.

Code	Packet Type	Code	Packet Type
1	Access-Request	4	Accounting-Request
2	Access-Accept	5	Accounting-Response
3	Access-Reject	11	Access-Challenge

- Identifier: Indicates the identifier for matching request packets and response packets, which occupies one byte. The identifier values of request packets and response packets of the same type are the same.

- Length: Identifies the length of a whole RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies two bytes. Bytes that are beyond the **Length** field will be truncated. If the length of a received packet is smaller than the value of **Length**, the packet is discarded.
- Authenticator: Verifies response packets of the RADIUS server by a RADIUS client, which occupies 16 bytes. This field is also used for encryption/decryption of user passwords.
- Attributes: Carries authentication, authorization, and accounting information, with the length unfixed. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Value (TLV) format. Type occupies one byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. Length occupies one byte and indicates the attribute length, with the unit of bytes. Value indicates the attribute information.

Attribute No.	Attribute Name	Attribute No.	Attribute Name
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry

Attribute No.	Attribute Name	Attribute No.	Attribute Name
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

Shared Key

A RADIUS client and a RADIUS server mutually confirm their identities by using a shared key during communication. The shared key cannot be transmitted over a network. In addition, user passwords are encrypted for transmission for the sake of security.

RADIUS Server Group

The RADIUS security protocol, also called RADIUS method, is configured in the form of a RADIUS server group. Each RADIUS method corresponds to one RADIUS server group and one or more RADIUS severs can be added to one RADIUS server group. For details about the RADIUS method, see the *Configuring AAA*. If you add multiple RADIUS servers to one RADIUS server group, when the communication between a device and the first RADIUS server in this group fails or the first RADIUS server becomes unreachable, the device automatically attempts to communicate with the next RADIUS server till the communication is successful or the communication with all the RADIUS servers fails.

RADIUS Attribute Type

- Standard attributes

The RFC standards specify the RADIUS attribute numbers and attribute content but do not specify the format of some attribute types. Therefore, the format of attribute contents needs to be configured to adapt to different RADIUS server requirements. Currently, the format of the RADIUS Calling-Station-ID attribute (attribute No.: 31) can be configured.

The RADIUS Calling-Station-ID attribute is used to identify user identities when a network device transmits request packets to the RADIUS server. The RADIUS Calling-Station-ID attribute is a string, which can adopt multiple formats. It needs to uniquely identify a user. Therefore, it is often set to the MAC address of a user. For example, when IEEE 802.1X authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the IEEE 802.1X client is installed. The following table describes the format of MAC addresses.

Format	Description
Ietf	Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC
Normal	Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac
Unformatted	Indicates the format without separators. This format is used by default. Example: 00d0f83322ac

- Private attributes

RADIUS is an extensible protocol. According to RFC2865, the Vendor-Specific attribute (attribute No.: 26) is used by device vendors to extend the RADIUS protocol to implement private functions or functions that are not defined in the standard RADIUS protocol. Table 1-3 lists private attributes supported by Ruijie products. The **TYPE** column indicates the default configuration of private attributes of Ruijie products and the **Extended TYPE** column indicates the default configuration of private attributes of other non-Ruijie products.

ID	Function	TYPE	Extended TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42

ID	Function	TYPE	Extended TYPE
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

Overview

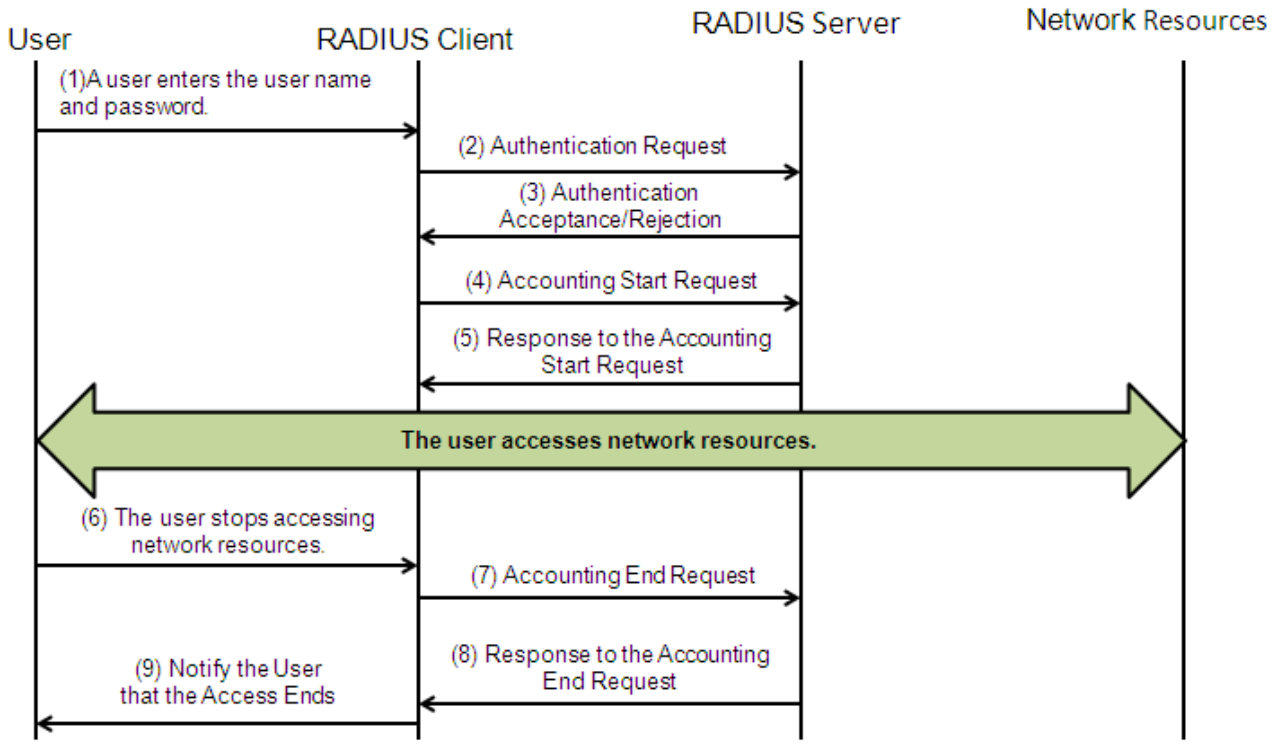
Feature	Description
RADIUS Authentication, Authorization, and Accounting	Conducts identity authentication and accounting on access users, safeguards network security, and facilitates management for network administrators.
Source Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Timeout Retransmission	Specifies the packet retransmission parameter for a RADIUS client when a RADIUS server does not respond to packets transmitted from the RADIUS client within a period of time.
RADIUS Server Accessibility Detection	Enables a RADIUS client to actively detect whether a RADIUS server is reachable and maintain the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.
RADIUS Forced Offline	Enables a RADIUS server to actively force authenticated users to go offline.

3.3.1 RADIUS Authentication, Authorization, and Accounting

Conduct identity authentication and accounting on access users, safeguard network security, and facilitate management for network administrators.

Working Principle

Figure 3-2



The RADIUS authentication and authorization process is described as follows:

8. A user enters the user name and password and transmits them to the RADIUS client.
9. After receiving the user name and password, the RADIUS client transmits an authentication request packet to the RADIUS server. The password is encrypted for transmission. For the encryption method, see RFC2865.
10. The RADIUS server accepts or rejects the authentication request according to the user name and password. When accepting the authentication request, the RADIUS server also issues authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

11. If the RADIUS server returns authentication acceptance information in Step (3), the RADIUS client sends an accounting start request packet to the RADIUS server immediately.
12. The RADIUS server returns the accounting start response packet, indicating accounting start.
13. The user stops accessing network resources and requests the RADIUS client to disconnect the network connection.
14. The RADIUS client transmits the accounting end request packet to the RADIUS server.
15. The RADIUS server returns the accounting end response packet, indicating accounting end.
16. The user is disconnected and cannot access network resources.

Related Configuration

Configuring RADIUS Server Parameters

No RADIUS server is configured by default.

You can run the **radius-server host** command to configure a RADIUS server.

At least one RADIUS server must be configured so that RADIUS services run normally.

Configuring the AAA Authentication Method List

No AAA authentication method list is configured by default.

You can run the **aaa authentication** command to configure a method list for different user types and select **group radius** when setting the authentication method.

The RADIUS authentication can be conducted only after the AAA authentication method list of relevant user types is configured.

Configuring the AAA Authorization Method List

No AAA authorization method list is configured by default.

You can run the **aaa authorization** command to configure an authorization method list for different user types and select **group radius** when setting the authorization method.

The RADIUS authorization can be conducted only after the AAA authorization method list of relevant user types is configured.

Configuring the AAA Accounting Method List

No AAA accounting method list is configured by default.

You can run the **aaa accounting** command to configure an accounting method list for different user types and select **group radius** when setting the accounting method.

The RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

3.3.2 Source Address of RADIUS Packets

Specify the source IP address used by a RADIUS client to transmit packets to a RADIUS server.

Working Principle

When configuring RADIUS, specify the source IP address to be used by a RADIUS client to transmit RADIUS packets to a RADIUS server, in an effort to reduce the workload of maintaining a large amount of NAS information on the RADIUS server.

Related Configuration

The global routing is used to determine the source address for transmitting RADIUS packets by default.

Run the **ip radius source-interface** command to specify the source interface for transmitting RADIUS packets. The device uses the first IP address of the specified interface as the source address of RADIUS packets.

3.3.3 RADIUS Timeout Retransmission

Working Principle

After a RADIUS client transmits a packet to a RADIUS server, a timer is started to detect the response of the RADIUS server. If the RADIUS server does not respond within a certain period of time, the RADIUS client retransmits the packet.

Related Configuration

↘ Configuring the RADIUS Server Timeout Time

The default timeout time is 5 seconds.

You can run the **radius-server timeout** command to configure the timeout time. The value ranges from 1 second to 1,000 seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout time according to actual conditions.

↘ Configuring the Retransmission Count

The default retransmission count is 3.

You can run the **radius-server retransmit** command to configure the retransmission count. The value ranges from 0 to 100.

↘ Configuring Whether to Retransmit Accounting Update Packets

Accounting update packets are not retransmitted by default.

You can run the **radius-server account update retransmit** command to configure retransmission of accounting update packets for authenticated users.

3.3.4 RADIUS Server Accessibility Detection

Working Principle

A RADIUS client actively detects whether a RADIUS server is reachable and maintains the accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve the handling performance of RADIUS services.

Related Configuration

↘ Configuring the Criteria for the Device to Judge That a RADIUS Server Is Unreachable

The default criteria configured for judging that a RADIUS server is unreachable meet the two conditions simultaneously: 1. The device does not receive a correct response packet from the RADIUS security server within 60 seconds. 2. The device transmits the request packet to the same RADIUS security server for consecutive 10 times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to judge that the RADIUS security server is unreachable.

↘ Configuring the Test User Name for Actively Detecting the RADIUS Security Server

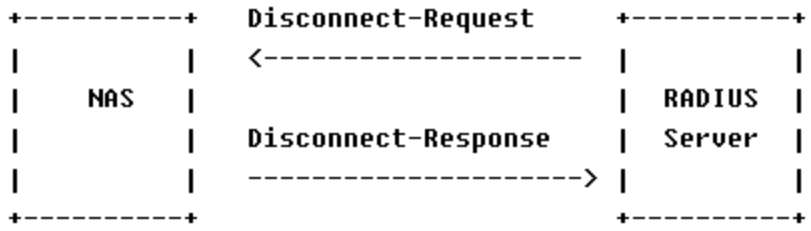
No test user name is specified for actively detecting the RADIUS security server by default.

You can run the **radius-server host x.x.x.xtestusername xxx** command to configure the test user name.

3.3.5 RADIUS Forced Offline

Working Principle

Figure 3-3 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol



The preceding figure shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP Port 3799 of the device. After processing, the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

3.3.6 Binding an Authentication Server

Working Principle

By binding a user to an authentication server, the user's authentication and accounting packets are sent to this server.

Related Configuration

↘ Binding an Authentication Server

Use the **radius-server account bind authen server** command to bind a user to an authentication server.

3.4 Configuration

Configuration	Description and Command	
RADIUS Basic Configuration	⚠ (Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.	
	radius-serverhost	Configures the IP address of the remote RADIUS security server.
	radius-serverkey	Configures the shared key for communication between the device and the RADIUS server.

Configuration	Description and Command	
	radius-serverretransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-servertimeout	Configures the waiting time, after which the device retransmits a request.
	radius-server account update retransmit	Configures retransmission of accounting update packets for authenticated users.
	ip radius source-interface	Configures the source address of RADIUS packets.
Configuring the RADIUS Attribute Type	(Optional) It is used to define attribute processing adopted when the device encapsulates and parses RADIUS packets.	
	radius-serverattribute31	Configures the MAC address format of RADIUS attribute No. 31 (Calling-Station-ID).
	radius-server attribute class	Configures the parsing mode of the RADIUS Class attribute.
	radius attribute	Configures the RADIUS private attribute type.
	radius set qoscos	Sets the private attribute port-priority issued by the server to the COS value of an interface. For COS-relevant concepts, see the *Configuring QoS*.
	radius support cui	Configures the device to support the CUI attribute.
	radius vendor-specific	Configures the mode of parsing private attributes by the device.
	radius vendor-specific attribute support	Configures whether the RADIUS server parses vendors' private attributes contained in packets.
Configuring RADIUS Accessibility Detection	(Optional) It is used to detect whether a RADIUS server is reachable and maintain the accessibility of the RADIUS server.	
	radius-server dead-criteria	Configures the global criteria for judging that a RADIUS security server is unreachable.
	radius-server deadtime	Configures the duration for the device to stop transmitting request packets to an unreachable RADIUS server.
	radius-server host	Configures the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.

3.4.1 RADIUS Basic Configuration

Configuration Effect

- RADIUS authentication, authorization, and accounting can be conducted after RADIUS basic configuration is complete.

Notes

- Before configuring RADIUS on the device, ensure that the network communication of the RADIUS server is in good condition.
- When running the **ip radius source-interface** command to configure the source address of RADIUS packets, ensure that the device of the source IP address communicates with the RADIUS server successfully.
- When conducting RADIUS IPv6 authentication, ensure that the RADIUS server supports RADIUS IPv6 authentication.

Configuration Steps

Configuring the Remote RADIUS Security Server

- Mandatory.
- Configure the IP address, authentication port, accounting port, and shard key of the RADIUS security server.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

- Optional.
- Configure a shared key in global configuration mode for servers without a shared key.

⚠ The shared key on the device must be consistent with that on the RADIUS server.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

- Optional.
- Configure the request transmission count, after which the device confirms that a RADIUS server is unreachable, according to the actual network environment.

Configuring the Waiting Time, After which the Device Retransmits a Request

- Optional.
- Configure the waiting time, after which the device retransmits a request, according to the actual network environment.

⚠ In an 802.1X authentication environment that uses the RADIUS security protocol, if a network device serves as the 802.1X authenticator and Ruijie SU is used as the 802.1X client software, it is recommended that **radius-server timeout** be set to 3 seconds (the default value is 5 seconds) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

- Optional.
- Determine whether to enable the function of retransmitting accounting update packets of authenticated users according to actual requirements.

Configuring the Source Address of RADIUS Packets

- Optional.
- Configure the source address of RADIUS packets according to the actual network environment.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to confirm that the device communicates with the RADIUS server over the RADIUS protocol.

Related Commands

Configuring the Remote RADIUS Security Server

Command	**radius-server host** [**oob**] { *ipv4-address* | *ipv6-address*} [**auth-port***port-number*] [**acct-port***port-number*][**test username***name* [**idle-time***time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]
Parameter Description	**oob**: Indicates oob authentication, that is, the source interface for transmitting packets to the RADIUS server is an mgmt port. *ipv4-address*: Indicates the IPv4 address of the RADIUS security server. *Ipv6-address*: Indicates the IPv6 address of the RADIUS security server. **auth-port***port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct identity authentication. **acct-port** *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to **0**, the host does not conduct accounting. **test username** *name*: Enables the function of actively detecting the RADIUS security server and specifies the user name used for active detection. **idle-time***time*: Indicates the interval for the device to transmit test packets to a reachable RADIUS security server. The default value is 60 minutes. The value ranges from 1 minute to 1,440 minutes (24 hours). **ignore-auth-port**: Disables the function of detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the function of detecting the accounting port of the RADIUS security server. It is enabled by default. **key**[**0** | **7**] *text-string* : Configures the shared key of the server. The global shared key is used if it is not configured.
Command Mode	Global configuration mode
Usage Guide	A RADIUS security server must be defined to implement the AAA security service by using RADIUS. You can run the **radius-server host** command to define one or more RADIUS security servers. If a RADIUS security server is not added to a RADIUS server group, the device uses the global routing table when transmitting RADIUS packets to the RADIUS server. Otherwise, the device uses the VRF routing table of the RADIUS server group.

Configuring the Shared Key for Communication Between the Device and the RADIUS Server

Command	**radius-server key** [**0** | **7**]*text-string*
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7**indicates simple encryption. The default value is **0**.
Command Mode	Global configuration mode
Usage Guide	A shared key is the basis for correct communication between the device and the RADIUS security server. The same shared key must be configured on the device and RADIUS security server so that they can communicate with each other successfully.

Configuring the Request Transmission Count, After Which the Device Confirms That a RADIUS Server Is Unreachable

Command	**radius-server retransmit***retries*
Parameter Description	*retries*: Indicates the RADIUS retransmission count. The value ranges from 0 to 100.
Command Mode	Global configuration mode
Usage Guide	The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count. There is an interval between consecutive two retransmissions.

Configuring the Waiting Time, After which the Device Retransmits a Request

Command	**radius-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the packet retransmission timeout time.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

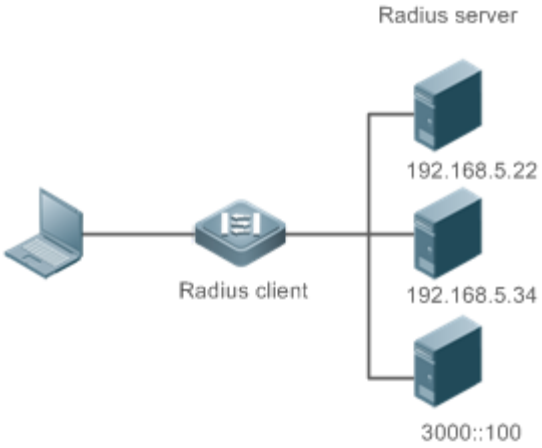
Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure retransmission of accounting update packets for authenticated users. Accounting update packets are retransmitted by default. The configuration does not affect users of other types.

Sending Accounting-On Packets After the NAS Device Restarts

Command	**radius-server accounting-on enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is run, Accounting-On packets are sent after the NAS device restarts. By default, this function is enabled. If you want to disable it, use the **no** form of this command.

Configuration Example

Using RADIUS Authentication, Authorization, and Accounting for Login Users

Scenario Figure 3-4	
Configuration Steps	● Enable AAA. ● Configure the RADIUS server information. ● Configure to use the RADIUS authentication, authorization, and accounting methods. ● Apply the configured authentication method on the interface.
RADIUS Client	`Ruijie#configure terminal` `Ruijie (config)#aaa new-model` `Ruijie (config)# radius-server host 192.168.5.22` `Ruijie (config)#radius-server host 3000::100` `Ruijie (config)# radius-server key aaa` `Ruijie (config)#aaa authentication login test group radius` `Ruijie (config)#aaa authorizationexectest group radius` `Ruijie (config)#aaa accountingexectest start-stop group radius`

	Ruijie (config)# line vty 0 4 Ruijie (config-line)#login authentication test Ruijie (config-line)# authorization exec test Ruijie (config-line)# accounting exec test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. After obtaining a certain access level granted by the server, only run commands under this access level. Display the authentication log of the user on the RADIUS server. Perform management operations on the device as the user and then log out. Display the accounting information on the user on the RADIUS server.
	Ruijie#show running-config ! radius-server host 192.168.5.22 radius-server host 3000::100 radius-server key aaa aaa new-model aaa accounting exec test start-stop group radius aaa authorization exec test group radius aaa authentication login test group radius no service password-encryption iptcp not-send-rst ! vlan 1 ! line con 0 line vty 0 4 accounting exec test authorization exec test login authentication test !

Common Errors

- The key configured on the device is inconsistent with that configured on the server.
- No method list is configured.

3.4.2 Configuring the RADIUS Attribute Type

Configuration Effect

- Define the attribute processing adopted when the device encapsulates and parses RADIUS packets.

Notes

- Private attributes involved in "Configuring the RADIUS Attribute Type" refer to Ruijie private attributes.

Configuration Steps

Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

- Optional.
- Set the MAC address format of **Calling-Station-Id** to a type supported by the server.

Configuring the Parsing Mode of the RADIUS Class Attribute

- Optional.
- Configure the parsing mode of the Class attribute according to the server type.

Configuring the RADIUS Private Attribute Type

- Optional.
- If the server is a Ruijie application server, the RADIUS private attribute type needs to be configured.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

- Optional.
- Set the private attribute **port-priority** issued by the server to the COS value of an interface as required.

Configures the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

Configuring the Mode of Parsing Private Attributes by the Device

- Optional.
- Configure the index of a Ruijie private attribute parsed by the device as required.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

- Optional.

- Configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Verification

- Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using RADIUS.
- Enable the device to interact with the RADIUS server. Conduct packet capture to display the MAC address format of Calling-Station-Id.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that Ruijie private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Display the debug information of the device to check that the CUI attribute is correctly parsed by the device.

Related Commands

↘ Configuring the MAC Address Format of RADIUS Attribute No. 31 (Calling-Station-ID)

Command	**radius-server attribute 31 mac format {ietf | normal | unformatted | dot-split | colon-split | hyphen-split} [mode1 | mode2] [lowercase | uppercase]**
Parameter Description	**ietf**: Indicates the standard format specified in the IETF standard (RFC3580), which is separated by the separator (-). Example: 00-D0-F8-33-22-AC. **normal**: Indicates the common format that represents a MAC address (dotted hexadecimal format), which is separated by the separator (.). Example: 00d0.f833.22ac. **unformatted**: Indicates the format without separators. This format is used by default. Example: 00d0f83322ac. **dot-split**: Indicates format representing the MAC address. '.'is used as the separator. This parameter should be configured with **mode1** or **mode2**. **colon-split**: Indicates format representing the MAC address. ':'is used as the separator. This parameter should be configured with **mode1** or **mode2**. **hyphen-split**: Indicates format representing the MAC address. '-'is used as the separator. This parameter should be configured with **mode1** or **mode2**. **mode1**: Indicates format representing the MAC address. Four characters make up one group. This parameter should be configured with **dot-split**, **colon-split**, or **hyphen-split**. For example: 00D0.F833.22AC, 00D0:F833:22AC, and 00D0-F833-22AC. **mode2**: Indicates format representing the MAC address. Two characters make up one group. This parameter should be configured with **dot-split**, **colon-split**, or **hyphen-split**. For example: 00.D0.F8.33.22.AC, 00:D0:F8:33:22:AC, and 00-D0-F8-33-22-AC. **lowercase**: Indicates lowercase letters to be used in the MAC address. **uppercase**: Indicates uppercase letters to be used in the MAC address.

Command Mode	Global configuration mode
Usage Guide	Some RADIUS security servers (mainly used for 802.1X authentication) can identify only MAC addresses in the IETF format. In this case, set the MAC address format of Calling-Station-ID to IETF.

Configuring the Parsing Mode of the RADIUS Class Attribute

Command	**radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**
Parameter Description	**user-flow-control:** Parses the rate limit configuration from the class attribute. **format-16bytes:** Sets the format of the rate limit value to 16 bytes in the **class** attribute. **format-32bytes:** Sets the format of the rate limit value to 32 bytes in the **class** attribute.
Command Mode	Global configuration mode
Usage Guide	Configure this command if the server needs to issue the rate limit value by using the Class attribute.

Configuring the RADIUS Private Attribute Type

Command	**radius attribute** { *id* | **down-rate-limit** | **dscp** | **mac-limit** | **up-rate-limit** } **vendor-type** *type*
Parameter Description	*id*: Indicates a function ID <1-255>. *type*: Indicates the private attribute type. **down-rate-limit**: Indicates the downstream rate limit. **dscp**: Indicates DSCP attribute. **mac-limit**: Indicates MAC-limit attribute. **up-rate-limit**: Indicates the upstream rate limit.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the RADIUS private attribute type.

Setting the Private Attribute port-priority Issued by the Server to the COS Value of an Interface

Command	**radius set qos cos**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to use the issued QoS value as the CoS value. The QoS value is used as the DSCP value by default.

Configures the Device to Support the CUI Attribute

Command	**radius support cui**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure this command to enable the RADIUS-compliant device to support the CUI attribute.

Configuring the Mode of Parsing Private Attributes by the Device

Command	**Radius vendor-specific extend**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to identify attributes of all vendor IDs by type.

Configuring Whether RADIUS Server Parses the Private Attribute of Cisco, Huawei or Microsoft

Command	**radius vendor-specific attribute support *vendor_name***
Parameter Description	*vendor_name*: Indicates the vendor name. It can be set to cisco, huawei or ms.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether RADIUS server parses the private attribute of Cisco, Huawei or Microsoft.

Configuration Example

Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	● Configure the MAC address format of RADIUS Calling-Station-Id. ● Configure the RADIUS private attribute type. ● Set the QoS value issued by the RADIUS server as the COS value of the interface. ● Configure the RADIUS function to support the CUI attribute. ● Configure the device to support private attributes of other vendors. ● Configure the RAIUDS server not to parse Cisoc's private attributes contained in packets.
	`Ruijie(config)#radius-server attribute 31 mac format ietf` `Ruijie(config)#radius attribute 16 vendor-type 211` `Ruijie(config)#radiussetqoscos` `Ruijie(config)#radiussupport cui`

	Ruijie(config)#radiusvendor-specific extend Ruijie(config)# no radius vendor-specific attribute support cisco
Verification	Conduct packet capture or display debug information of the device to check whether the RADIUS standard attributes and private attributes are encapsulated/parsed correctly.

3.4.3 Configuring RADIUS Accessibility Detection

Configuration Effect

The device maintains the accessibility status of each configured RADIUS server: reachable or unreachable. The device will not transmit authentication, authorization, and accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group as the unreachable server are all unreachable.

The device actively detects a specified RADIUS server. The active detection function is disabled by default. If the active detection function is enabled for a specified RADIUS server, the device will, according to the configuration, periodically transmits detection requests (authentication requests or accounting requests) to the RADIUS server. The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the active detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval is always 1 minute.

Notes

All the following conditions need to be met before the active detection function is enabled for a specified RADIUS server:

- The test user name of the RADIUS server is configured on the device.
- At least one tested port (authentication port or accounting port) of the RADIUS server is configured on the device.

If the following two conditions are all met, it is deemed that a reachable RADIUS server becomes unreachable:

- After the previous correct response is received from the RADIUS server, the time set in **radius-server dead-criteria time** *seconds* has elapsed.
- After the previous correct response is received from the RADIUS server, the count that the device transmits requests to the RADIUS server but fails to receive correct responses (including retransmission) reaches the value set in **radius-server dead-criteria tries** *number*.

If any of the following conditions is met, it is deemed that an unreachable RADIUS server becomes reachable:

- The device receives correct responses from the RADIUS server.
- The duration that the RADIUS server is in the unreachable state exceeds the time set in **radius-server deadtime** and the active detection function is disabled for the RADIUS server.
- The authentication port or accounting port of the RADIUS server is updated on the device.

Configuration Steps

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

- Mandatory.
- Configuring the global criteria for judging that a RADIUS security server is unreachable is a prerequisite for enabling the active detection function.

Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Active Detection Parameters

- Mandatory.
- Configuring active detection parameters of the RADIUS server is a prerequisite for enabling the active detection function.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

- Optional.
- The configured duration for the device to stop transmitting request packets to an unreachable RADIUS server takes effect only when the active detection function is disabled for the RADIUS server.

Verification

- Run the **show radius server** command to display the accessibility information of each RADIUS server.

Related Commands

Configuring the Global Criteria for Judging That a RADIUS Security Server Is Unreachable

Command	**radius-server dead-criteria** { **time***seconds* [**tries***number*] | **tries***number* }
Parameter Description	**time***seconds*: Indicates the time condition parameter. If the device fails to receive a correct response packet from a RADIUS security server within the specified time, it is deemed that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 second to 120 seconds. **tries***number*: Indicates the consecutive request timeout count. If the timeout count of request packets transmitted by the device to the same RADIUS security server reaches the preset count, it is deemed that the RADIUS security server meets the consecutive timeout count condition of inaccessibility. The value ranges from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	If a RADIUS security server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS security server is unreachable. Users can use this command to adjust parameter values in the duration condition and consecutive request timeout count condition.

Configuring the Duration for the Device to Stop Transmitting Request Packets to an Unreachable RADIUS Server

Command	**Radius-server deadtime** *minutes*

Parameter Description	*minutes*: Indicates the duration for the device to stop transmitting requests to an unreachable RADIUS security server, with the unit of minutes. The value ranges from 1 minute to 1,440 minutes (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the active detection function is enabled for a RADIUS security server on the device, the time parameter in **radius-server deadtime** does not take effect on the RADIUS server. If the active detection function is disabled for a RADIUS security server, the device automatically restores the RADIUS security server to the reachable state when the duration that the RADIUS security server is in the unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

↘ Configuring Accessibility Detection on the RADIUS Server

Scenario Figure 3-5	
Configuration Steps	● Configure the global criteria for judging that a RADIUS security server is unreachable. ● Configure the IP address of the remote RADIUS security server, authentication port, accounting port, and active detection parameters.
RADIUS Client	`Ruijie(config)#radius-server dead-criteria time120 tries 5` `Ruijie(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90`
Verification	Disconnect the network communication between the device and the server with the IP address of 192.168.5.22.Conduct RADIUS authentication through the device. After 120 seconds, run the **show radius server** command to check that the server state is **dead**.
	`Ruijie#show running-config` `…` `radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90` `radius-server dead-criteria time 120 tries 5` `…`

3.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears statistics of the RADIUS dynamic authorization extension function and restarts statistics.	**clear radius dynamic-authorization-extension statistics**

Displaying

Description	Command
Displays global parameters of the RADIUS server.	**show radius parameter**
Displays the configuration of the RADIUS server.	**show radius server**
Displays the configuration of the RADIUS private attribute type.	**show radius vendor-specific**
Displays statistics relevant to the RADIUS dynamic authorization extension function.	**show radius dynamic-authorization-extension statistics**
Displays statistics relevant to RADIUS authentication.	**show radius auth statistics**
Displays statistics relevant to RADIUS accounting.	**show radius acct statistics**
Displays configuration of RADIUS server groups.	**show radius group**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the RADIUS event.	**debugradiusevent**
Debugs RADIUS packet printing.	**debugradiusdetail**
Debugs the RADIUS dynamic authorization extension function.	**debug radiusextension event**
Debugs the RADIUS dynamic authorization extension packet printing.	**debug radius extension detail**

4 Configuring 802.1X

4.1 Overview

IEEE 802.1X is a standard for port-based network access control that provides secure access service for local area networks (LANs).

In IEEE 802-compliant LANs, users connecting to the network access devices (NASs) can access network resources without authentication and authorization, bringing security risks to the network. IEEE 802.1X was proposed to resolve security problems of such LANs.

802.1X supports three security applications: authentication, authorization, and accounting, which are called AAA.

- Authentication: Checks whether to allow user access and restricts unauthorized users.
- Authorization: Grants specified services to users and controls permissions of authorized users.
- Accounting: Records network resource status of users to provide statistics for charges.

802.1X can be deployed in a network to realize user authentication, authorization and other functions.

Protocols and Standards

- IEEE 802.1X: Port-Based Network Access Control

4.2 Applications

Application	Description
Wireless 802.1X Authentication	When an enterprise deploys a wireless LAN (WLAN), 802.1X authentication should be enabled on the Access Controller (AC).

4.2.1 Wireless 802.1X Authentication

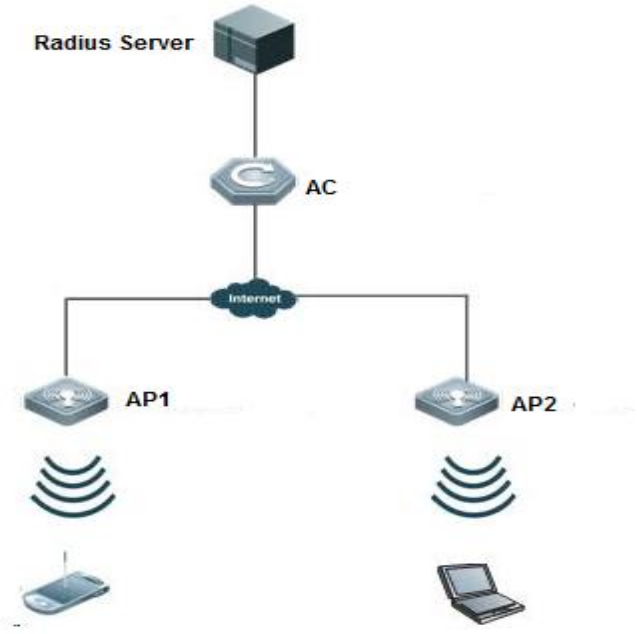
Scenario

An enterprise deploys a fit-AP wireless authentication environment including fit Access Points (APs) and an AC. 802.1X is deployed for secure admission. Wireless stations or devices (STAs) should pass 802.1X authentication to access the enterprise network.

As shown in Figure 4-1:

- STAs are installed with 802.1X clients (which can come with the operating system, or others like Ruijie Supplicant).
- The AC supports 802.1X.
- One or multiple RADIUS servers perform authentication.

Figure 4-1



Remarks	STAs support 802.1X authentication. After connecting to APs, they will be authenticated through 802.1X. 802.1X authentication is enabled on the AC. The RADIUS server runs the RADIUS server software to perform identity verification.

Deployment

- Enable 802.1X authentication on the AC based on the WLANs broadcast by APs to make associated STAs controlled. Only authenticated STAs can access the network.
- Configure an AAA authentication method list so that 802.1X can adopt the appropriate method and authentication server.
- Configure RADIUS parameters to ensure proper communication between the AC and the RADIUS server. For details, see the *Configuring RDS*.
- If a Ruijie RADIUS server is used, configure SNMP parameters to allow the RADIUS server to manage devices, such as querying and setting.
- Create an account on the RADIUS server, register the IP addresses of the AC, and configure RADIUS-related parameters. Only in this case, can the RADIUS server respond to the requests of the AP/AC.

4.2.2 MAB Auto Authentication

Scenario

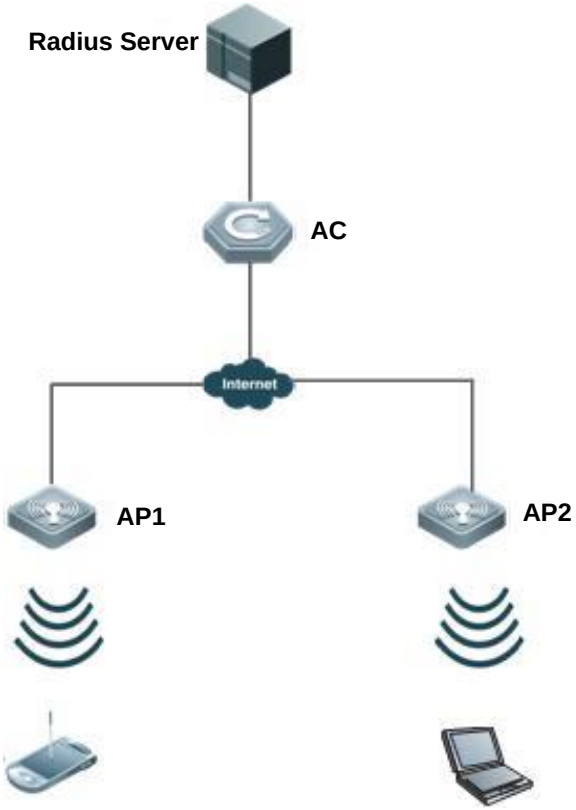
MAC address bypass (MAB) auto authentication indicates that MAB authentication is performed together with Web authentication. In the original wireless Web authentication scenario, it is complained that the ease-to-use performance of Web authentication is poor. During each Web authentication, a user needs to associate the STA with an SSID, open the

browser, and enter the user name and password. In addition, if the STA drops out of the network, the STA cannot automatically access the network again. To ensure that all Web authenticated STAs are always online and access the network imperceptibly, MAB auto authentication is proposed. After a STA passes Web authentication, the STA can access the network again imperceptibly without Web authentication.

As shown in Figure 4-2

- Only the browser is mandatory on the client.
- The AC supports Web authentication and MAB authentication.
- One or multiple RADIUS servers provide authentication. In addition, the authentication server supports the authentication mode of using the MAC address as the user name and password.

Figure 4-2



Remarks	Wireless MAB authentication is triggered by a STA advertisement. When a STA is already online, MAB authentication will not be triggered again. If MAB authentication fails, it can be triggered again only after the STA goes offline and reconnects to the network.

Deployment

- Enable Web authentication, DOT1X authentication, and MAB authentication on the interface of the AC. MAB authentication can be performed only after DOT1X authentication is enabled. (For details about MAB authentication,

see section **4.4.4** "**Configuring MAB** Auto Authentication". For details about Web authentication, see the WEB-AUTH-SCG document.)

- Configure an AAA authentication method list, so that a correct method and authentication server can be used for MAB/Web authentication. (For details about the AAA authentication method list configuration, see the AAA-SCG document.)
- Configure RADIUS parameters to ensure proper communication between the AC and the RADIUS server. In addition, configure the RADIUS server to support the authentication mode of using the MAC address as the user name and password. For details about the RADIUS configuration, see the corresponding configuration guide.
- If a Ruijie RADIUS server is used, configure SNMP parameters to allow the RADIUS server to perform operations such as querying and setting on the AP.
- Create an account on the RADIUS server, register the IP address of the AC, and configure RADIUS-related parameters. The RADIUS server can respond to the requests of the AP and AC only after the foregoing settings are completed.

4.3 Features

Basic Concepts

User

802.1X is a LAN-based protocol. It identifies users based on physical information but not accounts. Except them, all other information such as the account ID and IP address can be changed. In WLANs, one MAC address represents an STA.

RADIUS

RADIUS is a remote authentication protocol defined in RFC2865, which get wide practice. Using this protocol, the authentication server can remotely deploy and perform authentication. During 802.1X deployment, the authentication server is remotely deployed, and 802.1X authentication information between the NAS and the authentication server is transmitted through RADIUS.

Timeout

During authentication, an NAS needs to communicate with the authentication client and server. If the authentication client or server times out, not responding within the time specified by 802.1X, authentication will fail. During deployment, ensure that the timeout specified by 802.1X is longer than that specified by RADIUS.

MAB

MAC address bypass (MAB) authentication means that the MAC address is used as the user name and password for authentication. Since Ruijie Supplicant cannot be installed on some dumb ends such as network printers, use MAB to perform security control.

EAP

802.1X uses Extensible Authentication Protocol (EAP) to carry authentication information. Defined in RFC3748, EAP provides a universal authentication framework, in which multiple authentication modes are embedded, including Message Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Transport Layer Security (TLS). Ruijie 802.1X authentication supports various modes including MD5, CHAP, PAP, PEAP-MSCHAP, and TLS.

Authorization

Authorization means to bind specified services to authenticated users, such as VLAN and Access Control List (ACL).

Accounting

Accounting performs network audit on network usage duration and traffic for users, which facilitates network operation, maintenance, and management.

Some RADIUS servers such as RG-SAM\RG-SMP servers need to check the online/offline status based on accounting packets. Therefore, accounting must be enabled on these RADIUS servers.

Overview

Feature	Description
Authentication	Provides secure admission for users. Only authenticated users can access the network.
Authorization	Grants network access rights to authenticated users, such as IP address binding and ACL binding
Accounting	Provides online record audit, such as online duration and traffic.

4.3.1 Authentication

Authentication aims to check whether users are authorized and prevent unauthorized users from accessing the network. Users must pass authentication to obtain the network access permission. They can access the network only after the authentication server verifies the account. Before user authentication succeeds, only EAPOL packets (Extensible Authentication Protocol over LAN, 802.1X packets) can be transmitted over the network for authentication.

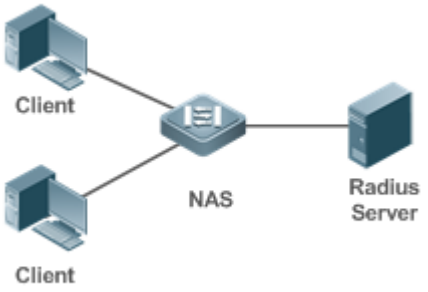
Working Principle

802.1X authentication is very simple. After a user submits its account information, the NAS sends the account information to the remote RADIUS server for identity authentication. If the authentication succeeds, the user can access the network.

Roles in Authentication

802.1X authentication involves three roles: supplicant, authenticator, and server. In real applications, their respective roles are client, network access server (NAS), and authentication server (mostly RADIUS server).

Figure 4-3



- Supplicant

The supplicant is the role of end users, usually a PC. It requests to access network services and replies to the request packets of the authenticator. The supplicant must run software compliant with the 802.1X standard. Except the typical 802.1X client support embedded in the operating system, Ruijie has launched a Ruijie Supplicant compliant with the 802.1X standard.

- Authenticator

The authenticator is usually an NAS such as a switch or wireless access hotspot. It controls the network connection of a client based on the client's authentication status. As a proxy between the client and the authentication server, the authenticator requests the user name from the client, verifies the authentication information from the authentication server, and forwards it to the client. Except as the 802.1X authenticator, the so-called NAS also acts as a RADIUS Client. It encapsulates the replies of the client into the RADIUS-format packets and forwards the packets to the RADIUS server. After receiving the information from the RADIUS server, it interprets the information and forwards it to the client.

The authenticator has two types of ports: controlled port and uncontrolled port. Users connected to controlled ports can access network resources only when authenticated. Users connected to uncontrolled ports can directly access network resources without authentication. We can connect users to controlled ports to control users. Uncontrolled ports are mainly used to connect the authentication server to ensure proper communication between the authentication server and the NAS.

- Authentication server

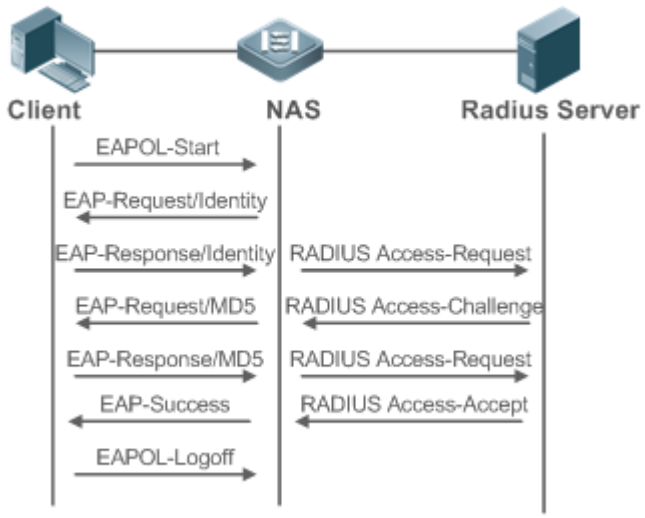
The authenticator server is usually an RADIUS server. It cooperates with the authenticator to provide authentication service for users. The authentication server saves the user names, passwords, and related authorization information. One server can provides authentication service for multiple authenticators to achieve centralized user management. The authentication server also manages accounting data received from authenticators. Ruijie RADIUS servers compliant with 802.1X standard include Microsoft IAS/NPS, Free RADIUS Server, and Cisco ACS.

↘ Authentication Process and Packet Exchange

The supplicant exchanges information with the authenticator through EAPOL while exchanges information with the authentication server through RADIUS. EAPOL is encapsulated on the MAC layer, with the type number of 0x888E. IEEE assigned a multicast MAC address 01-80-C2-00-00-03 for EAPOL to exchange packets during initial authentication. Ruijie Supplicant may also use 01-D0-F8-00-00-03 to for initial authentication packets.

Figure 4-4 shows the typical authentication process of a wired user.

Figure 4-4



This is a typical authentication process initiated by a user. In special cases, the NAS, may take place of the user to initiate an authentication request.

Authenticating User Status

802.1X determines whether a user on a port can access the network based on the authentication status of the port. Ruijie products extend the 802.1X and realizes access control based on users (identify a wired user by the MAC address and VLAN ID while an STA by the MAC address) by default. Ruijie 802.1X can also be enabled in interface configuration mode. For details, see the chapter "Configuration."

All users on an uncontrolled port can access network resources, while users on a controlled port can access network resources only after authorized. When a user initiates authentication, its status remains Unauthorized and cannot access the network yet. After it passes authentication, its status changes to Authorized and can access network resources.

If the user connected to a controlled port does not support 802.1X, it will not respond to the NAS requesting the user name of the user. That means, the user remains Unauthorized and cannot access network resources.

In the case of 802.1X-enabled user and 802.1X-disabled NAS, if the user does not receive any responses after sending a specified number of EAPOL-Start packets, it regards the connected port uncontrolled and directly accesses network resources.

On 802.1X-enabled devices, all ports are uncontrolled by default. We can configure a port as controlled so that all users on this port have to be authorized.

If a user passes authentication (that is, the NAS receives a success packet from the RADIUS server), the user becomes Authorized and can freely access network resources. If the user fails in authentication, it remains Unauthorized and re-initiates authentication. If the communication between the NAS and the RADIUS server fails, the user remains Unauthorized and cannot access network resources.

When a user sends an EAPOL-LOGOFF packet, the user's status changes from Authorized to Unauthorized.

When the NAS restarts, all users on it become Unauthorized.

If you want to forcibly make a client free from authentication, it is recommended to add a static MAC address.

↘ Deploying the Authentication Server

802.1X authentication uses the RADIUS server as the authentication server. Therefore, when 802.1X secure admission is deployed, the RADIUS server also needs to be deployed. Common RADIUS servers include Microsoft IAS/NPS, Cisco ACS, and RG-SAM/SMP. For details about the deployment procedure, see related software description.

↘ Configuring Authentication Parameters

To use 802.1X authentication, enable 802.1X authentication on the access port and configure AAA authentication method list and RADIUS server parameters. To ensure the accessibility between the NAS and RADIUS server, the 802.1X server timeout should be longer than the RADIUS server timeout.

↘ Supplicant

A user should start Ruijie Supplicant to enter the user name and initiate authentication. If the operating system brings an own authentication client and the network is available, a dialog box will be displayed, asking the user to enter the user name. Different clients may have different implementation processes and Graphical User Interfaces (GUIs). It is recommended to use Ruijie Supplicant as the authentication client. If other software is used, see related software description.

↘ Offline

If a user does not want to access the network, it can choose to go offline by multiple approaches, such as powering off the device, connecting the port to the network, and offline function provided by some supplicants.

↘ VLAN Hopping

After passing 802.1X authentication, a user is added to the VLAN assigned by the server. Then the user is allowed to communicate within that VLAN.

4.3.2 Authorization

After a user passes authentication, the NAS restricts the accessible network resources of the user in multiple approaches, such as accessible VLANs

Working Principle

Authorization means to bind the permissions with the users. A user is identified based on the MAC address and VLAN ID, as mentioned before. Besides MAC-VID binding, some other information such as the IP address and VLAN ID are bound with a user to implement authorization.

↘ ACL Authorization

After user authentication is complete, the authentication server delivers the ACL or ACE to users. The ACL must be configured on the authentication server before delivery while no extra configuration is required for ACE delivery. ACL

authorization delivers the ACL based on RADIUS attributes such as standard attributes, Ruijie-proprietary attributes, and Cisco-proprietary attributes. For details, see the software description related to the RADIUS server.

Kickoff

Used with RG-SAM/SMP, Ruijie 802.1X server can kick off online users who will be disconnected with the network. This function applies to the environment where the maximum online period and real-time accounting check function are configured.

4.3.3 Accounting

Accounting allows the network operators to audit the network access or fees of accessed users, including the online time and traffic.

Working Principle

Accounting is enabled on the NAS. The RADIUS server supports RFC2869-based accounting. When a user goes online, the NAS sends an accounting start packet to the RADIUS server which then starts accounting. When the user goes offline, the NAS sends an accounting end packet to the RADIUS server which then completes the accounting and generates a network fee accounting list. Different servers may perform accounting in different ways. Moreover, not all servers support accounting. Therefore, refer to the usage guide of the authentication server during actual deployment and accounting.

Accounting Start

After a user passes authentication, the accounting-enabled switch sends the RADIUS server an accounting start packet carrying user accounting attributes such as user name and accounting ID. After receiving the packet, the RADIUS server starts accounting.

Accounting Update

The NAS periodically sends Accounting Update packets to the RADIUS server, making the accounting more real-time. The accounting update interval can be provided by the RADIUS server or configured on the NAS.

Accounting End

After a user goes offline, the NAS sends the RADIUS server an accounting end packet carrying the online period and traffic of the user. The RADIUS server generates online records based on the information carried in this packet.

4.4 Configuration

Configuration	Description and Command	
Configuring 802.1X Basic Functions	⚠ (Mandatory) It is used to configure basic authentication and accounting.	
	aaa new-model	Enables AAA.
	aaa authentication dot1x	Configures an AAA authentication method list.

	aaa accounting networks	Configures an AAA accounting method list.
	radius-server host	Configures the RADIUS server parameters.
	radius-server key	Configures the preshared key for communication between the NAS and the RADIUS server.
Configuring 802.1X Parameters	(Optional) It is used to configure 802.1X parameters. Ensure that the 802.1X server timeout is longer than the RADIUS server timeout. Online Ruijie client detection applies only to Ruijie Supplicant.	
	dot1x re-authentication	Enables re-authentication.
	dot1x timeout re-authperiod	Configures the re-authentication interval.
	dot1x timeout tx-period	Configures the interval of EAP-Request/Identity packet retransmission.
	dot1x reauth-max	Configures the maximum times of EAP-Request/Identity packet retransmission.
	dot1x timeout supp-timeout	Configures the interval of EAP-Request/Challenge packet retransmission.
	dot1x max-req	Configures the maximum times of EAP-Request/Challenge packet retransmission.
	dot1x timeout server-timeout	Configures the authentication server timeout.
	dot1x timeout quiet-period	Configures the quiet period after authentication fails.
	dot1x auth-mode	Specifies the authentication mode (EAP/CHAP/PAP).
Configuring MAB	(Optional) It is used to configure MAC Authentication Bypass (MAB). MAB adopts the PAP authentication mode. Ensure correct server configurations during deployment.	
	dot1x mab	Configures wireless MAB.
	dot1x mab-username upper	Enables uppercase letters in MAB user names.

<table>
<tr><td rowspan="9">Configuring Extended Functions</td><td colspan="2">(Optional) It is used to configure active authentication requests on a port.
(Optional) It is used to configure the authenticated client list.
(Optional) It is used to enable 802.1X packet sending with the pseudo source MAC address.
(Optional) It is used to configure multiple accounts for the same MAC address.</td></tr>
<tr><td>dot1x multi-account enable</td><td>Enables multi-account authentication with one MAC address.</td></tr>
<tr><td>dot1x valid-ip-acct enable</td><td>Enables IP-triggered accounting.</td></tr>
<tr><td>dot1x valid-ip-acct timeout</td><td>Configures the timeout of obtaining IP addresses after users get authenticated. If timeout is reached, they will be kicked off.</td></tr>
<tr><td>dot1x event server-invalid action bypass-wlan</td><td>Configures the bypass WLAN for the RADIUS server.</td></tr>
<tr><td>dot1x encryption only</td><td>Configures 802.1X authentication for encryption only when 802.1X and Web authentication are both enabled.</td></tr>
<tr><td>dot1x logging rate-limit</td><td>Limits the rate of printing online and offline logs.</td></tr>
<tr><td>dot1x offline-detect</td><td>Enables traffic detection on users in WLAN.</td></tr>
<tr><td>dot1x user-trap enable</td><td>Enables SNMP trap during online and offline.</td></tr>
</table>

4.4.1 Configuring 802.1X Basic Functions

Configuration Effect

- Enable basic authentication and accounting services.
- On a wired network, run the **dot1x port-control auto** command in interface configuration mode to enable 802.1X authentication on a port.
- Run the **radius-server host** *ip-address* command to configure the IP address and port information of the RADIUS server and the **radius-server key** command to configure the RADIUS communication key between the NAS and the RADIUS server to ensure secure communication.
- Run the **aaa accounting update** command in global configuration mode to enable accounting update and the **aaa accounting update interval** command on the NAS to configure the accounting update interval. If the RADIUS server supports accounting update, you can also configure it on the RADIUS server. Prefer to use the parameters assigned by the authentication server than the parameters configured on the NAS.

Notes

- Configure accurate RADIUS parameters so that the basic RADIUS communication is proper.

- The 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, errors may occur during authentication and accounting.
- 802.1X uses the default method list by default. If the default method list is not configured for AAA, run the **dot1x authentication** and **dot1x accounting** commands to reconfigure the it.
- When RG-SAM/SMP is used, accounting must be enabled. Otherwise, the RADIUS server will fail to detect users going offline, causing offline users remaining in the online user table.

Configuration Steps

Enabling AAA

- (Mandatory) 802.1X authentication and accounting take effect only after AAA is enabled.
- Enable AAA on the NAS that needs to control user access by 802.1X.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	AAA is disabled by default.
Command Mode	Global configuration mode
Usage Guide	AAA is disabled by default. This command is mandatory for the deployment of 802.1X authentication.

Enabling an AAA Authentication Method List

- Mandatory.
- The AAA authentication method list must be consistent with the 802.1X authentication method list.
- Enable an AAA authentication method list after 802.1X authentication is enabled on the NAS.

Command	**aaa authentication dot1x** *list-name* **group radius**
Parameter Description	*list-name*: Indicates the 802.1X authentication method list of AAA.
Defaults	No AAA authentication method list is configured by default.
Command Mode	Global configuration mode
Usage Guide	AAA authentication modes are disabled by default. The AAA authentication mode must be consistent with the 802.1X authentication mode.

Configuring the RADIUS Server Parameters

- (Mandatory) The RADIUS server parameters must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure RADIUS server parameters after 802.1X authentication is enabled on the NAS.

Command	**radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description	*ip-address*: Indicates the IP address of the RADIUS server. *port1*: Indicates the authentication port. *port2*: Indicates the accounting port.
Defaults	No RADIUS server parameters are configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Preshared Key for Communication between the NAS and RADIUS Server

- (Mandatory) The preshared key for communication between the NAS and RADIUS server must be configured to ensure proper communication between the NAS and the RADIUS server.
- Configure the preshared key of the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**radius-server key** *string*
Parameter Description	*string*: Indicates the preshared key.
Defaults	No preshared key is configured for communication between the NAS and RADIUS server by default.
Command Mode	Global configuration mode
Usage Guide	The IP address of the NAS must be the same as that registered on the RADIUS server. The preshared key on the NAS must be the same as that on the RADIUS server. If the default RADIUS communication ports are changed on the RADIUS server, you need to change the communication ports on the NAS correspondingly.

Enabling 802.1X on a Port

- This command is mandatory for a wired network.
- Enable 802.1X on switches.

Command	**dot1x port-control auto**
Parameter Description	N/A
Defaults	802.1X is disabled on a port by default.
Command Mode	Interface configuration mode, VxLAN mode
Usage Guide	802.1X is disabled on a port by default. This command is mandatory for the deployment of 802.1X authentication. The default method list is used by default. If the 802.1X authentication method list in AAA is not the default one, the configured 802.1X authentication method list should match.

Enabling 802.1X

- This function is mandatory in a wireless network.

- Enable 802.1X on an AC or AP.
- If 802.1X is enabled on a WLAN, only 802.11 management frames and EAP packets are allowed to pass.
- For related commands, see the *Configuring RSNA*.

Verification

Start Ruijie Supplicant, enter the correct account information, and initiate authentication. Then check whether the 802.1X and RADIUS configurations are correct.

Checking for 802.1X Authentication Entries

Command	**show dot1x summary**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display entries of authenticated users to check the authentication status of users, for example, authenticating, authenticated, or quiet. Up to 30 characters are allowed to be contained in the “username” field, and the part after the 30th character is not displayed.
Command Display	Ruijie#show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-state Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16777302 ts-user b048.7a7f.f9f3 wlan 1 1 Authenticated Idle Authed static 0days 0h 0m12s

Checking for AAA User Entries

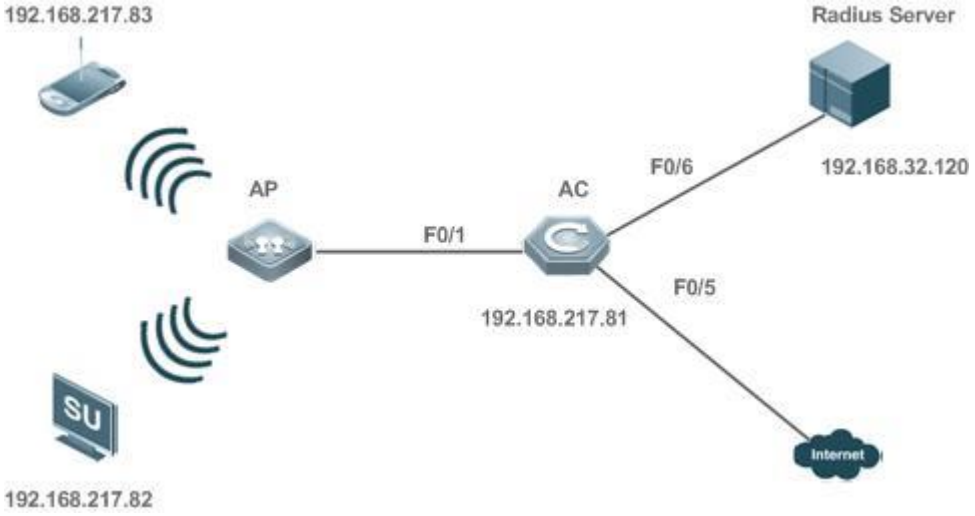
Command	**show aaa user all**
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Display information of AAA users.
Command Display	Ruijie#show aaa user all --- Id ----- Name 2345687901 wwxy ---

- Check whether the RADIUS server responds to authentication based on the RADIUS packets between the NAS and the RADIUS server. If no, it means that the network is disconnected or parameter configurations are incorrect. If the

RADIUS server directly returns a rejection reply, check the log file on the RADIUS server to identify the cause, e.g., of the authentication mode of the authentication server is incorrectly configured.

Configuration Example

Configuring 802.1X Authentication on a WLAN

Scenario **Figure 4-5**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication on ports of the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	`ruijie# configure terminal` `ruijie (config)# aaa new-model` `ruijie (config)# radius-server host 192.168.32.120` `ruijie (config)# radius-server key ruijie` `ruijie (config)# wlansec 1` `Ruijie(config-wlansec)# security rsn enable` `Ruijie(config-wlansec)# security rsn ciphers aes enable` `Ruijie(config-wlansec)# security rsn akm 802.1x enable`
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username:tests-user,password:test**. ● The user fails to ping 192.168.32.120 before authentication.

	• After the user enters account information and click **Authenticate** on Ruijie Supplicant, the authentication succeeds and the user can successfully ping 192.168.32.120. • Information of the authenticated user is displayed. `ruijie# show dot1x summary` `ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time` `--- --- --- --- --- --- --- --- --- ---` `16778217 ts-user 0023.aeaa.4286 wlan 1 2 Authenticated Idle Authed static 0days 0h 0m 7s`

Common Errors

- RADIUS parameters are incorrectly configured.
- The RADIUS server has a special access policy, for example, the RADIUS packets must carry certain attributes.
- The AAA authentication mode list is different from the 802.1X authentication mode list, causing authentication failure.

4.4.2 Configuring 802.1X Parameters

Configuration Effect

- Adjust 802.1X parameter configurations based on the actual network situation. For example, if the authentication server has poor performance, you can raise the authentication server timeout.

Notes

- 802.1X and RADIUS have separate server timeouts. By default, the authentication server timeout of 802.1X is 5 seconds while that of RADIUS is 15 seconds. In actual situations, ensure that the former is greater than the latter. You can run the **dot1x timeout server-timeout** command to adjust the authentication server timeout of 802.1X. For detailed configuration about the RADIUS server timeout, see the *Configuring RADIUS*.

Configuration Steps

↘ Enabling Re-authentication

- (Optional) After re-authentication is enabled, the NAS can periodically re-authenticate online users.
- Enable re-authentication after 802.1X authentication is enabled on the NAS.

Command	**dot1x re-authentication**
Parameter Description	N/A
Defaults	Re-authentication is disabled by default.
Command Mode	Global configuration mode

Usage Guide	You can run this command to periodically re-authenticate users.

Configuring the Re-authentication Interval

- (Optional) You can configure the re-authentication interval for users.
- Configure the re-authentication interval after 802.1X authentication is enabled on the NAS. The re-authentication interval takes effect only after re-authentication is enabled.

Command	**dot1x timeout re-authperiod** *period*
Parameter Description	*period*: Indicates the re-authentication interval in the unit of seconds.
Defaults	The default value is 3,600 seconds.
Command Mode	Global configuration mode
Usage Guide	Adjust the re-authentication interval as required.

Configuring the Interval of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates a longer interval of packet retransmission.
- Configure the interval of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout tx-period** *period*
Parameter Description	*period*: Indicates the interval of EAP-Request/Identity packet retransmission in the unit of seconds.
Defaults	The default value is 3 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Adjust the value based on how long the authentication client responds to the NAS's requests.

Configuring the Maximum Times of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Identity packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x reauth-max** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Identity packet retransmission.
Defaults	The default value is 3 for switches while 6 for wireless devices.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. In the case of high-rate packet loss, increase this value so that the clients can easily receive packets from the NAS.

Configuring the Interval of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates a longer retransmission interval.
- Configure the interval of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout supp-timeout** *time*
Parameter Description	*time*: Indicates the interval of EAP-Request/Challenge packet transmission in the unit of seconds.
Defaults	The default value is 3 seconds for switches while 4 seconds for wireless devices.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Maximum Times of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates more frequent retransmissions.
- Configure the maximum times of EAP-Request/Challenge packet retransmission after 802.1X authentication is enabled on the NAS.

Command	**dot1x max-req** *num*
Parameter Description	*num*: Indicates the maximum times of EAP-Request/Challenge packet retransmission in the unit of seconds.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Optional. It is recommended to use the default value. Increase this value in the case of high-rate packet loss.

Configuring the Authentication Server Timeout

- (Optional) A larger value indicates a longer authentication server timeout.
- Configure the authentication server timeout after 802.1X authentication is enabled on the NAS.
- The server timeout of RADIUS must be greater than that of 802.1X.

Command	**dot1x timeout server-timeout** *time*
Parameter Description	*time*: Indicates the authentication server timeout in the unit of seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value if the communication between the NAS and RADIUS server is unstable.

Configuring the Quiet Period after Authentication Fails

- (Optional) A larger value indicates a longer quiet period.
- Configure the quiet period after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout quiet-period** *time*
Parameter Description	*time*: Indicates the quiet period after authentication fails. The unit is second.
Defaults	The default value is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Increase this value to prevent users from frequently initiating authentication to the RADIUS server, thereby reducing the load of the authentication server.

Specifying the Authentication Mode

- (Optional) Configure the mode for 802.1X authentication.
- Configure the authentication mode after 802.1X authentication is enabled on the NAS.

Command	**dot1x auth-mode** {**eap** | **chap** | **pap**}
Parameter Description	**eap**: Indicates EAP authentication. **chap**: Indicates CHAP authentication. **pap**: Indicates PAP authentication.
Defaults	The default value is **eap**.
Command Mode	Global configuration mode
Usage Guide	Select the authentication mode supported by Ruijie Supplicant and authentication server.

Verification

Run the **show dot1x** command to check whether parameter configurations take effect.

Configuration Example

Specifying the Authentication Mode

Scenario	The NAS is deployed in standalone mode.
Configuration Steps	Set the authentication mode to **chap**.
	`Ruijie(config)#dot1x auth-mode chap`
Verification	Display the configurations. `Ruijie(config)#show dot1x` `802.1X basic information:`

```
802.1X Status ..................... enable
Authentication Mode ................ chap
Authorization mode ................. disable
Total User Number .................. 0 (exclude dynamic user)
Authenticated User Number ........... 0 (exclude dynamic user)
Dynamic User Number ................ 0
Re-authentication .................. disable
Re-authentication Period ........... 3600 seconds
Re-authentication max .............. 3 times
Quiet Period ....................... 10 seconds
Tx Period .......................... 30 seconds
Supplicant Timeout ................. 3 seconds
Server Timeout ..................... 5 seconds
Maximum Request .................... 3 times
Client Online Probe ................ disable
Eapol Tag .......................... disable
802.1x redirect .................... disable
Private supplicant only ............ disable
```

Common Errors

- The server timeout is shorter than the RADIUS timeout.

4.4.3 Configuring MAB

Configuration Effect

- On WLANs, WLAN-based MAB is supported. If MAB is enabled, the NAS automatically associates the MAC address of an STA on the WLAN as the user name and password to initiate authentication to the authentication server.

Notes

- If MAB is enabled on a WLAN, set the WLAN security mode to OPEN.

Configuration Steps

↘ Enabling WLAN-based MAB

- Optional.
- Enable MAB on the WLAN connected to STAs.

Command	dot1x-mab
Parameter Description	N/A
Defaults	WLAN-based MAB is disabled by default.

Command Mode	WLAN security configuration mode
Usage Guide	Run this command when STAs on a WLAN need to perform authentication using MAC addresses. This command applies only to wireless devices.

Enabling Uppercase Letters in MAB User Names

- Optional.
- Enable this function in global configuration mode.

Command	**dot1x mab-username upper**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.

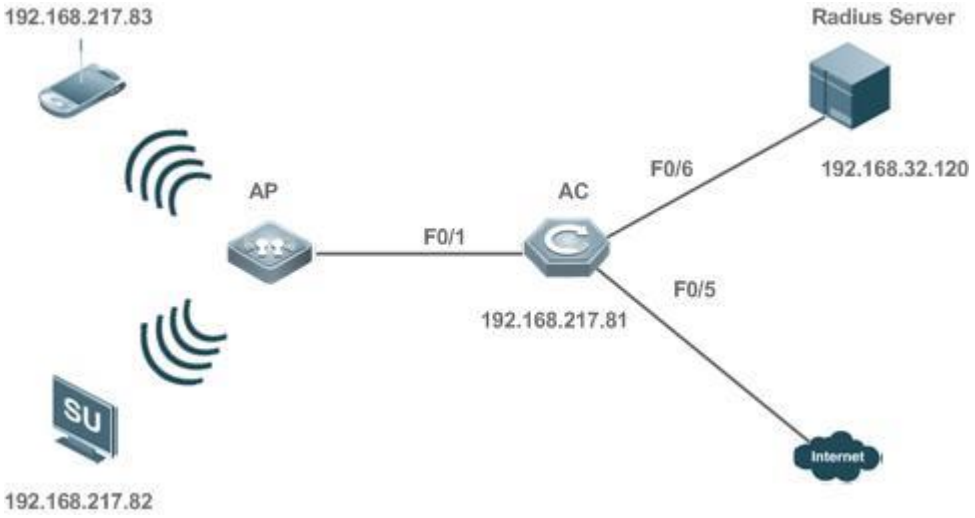
Verification

Check whether the dumb user can access the network. If yes, MAB takes effect. If no, MAB does not take effect.

- Check whether MAB functions are configured on the authentication server and NAS.
- Check whether dumb users with illegitimate MAC addresses cannot access the network.
- Check whether dumb users with illegitimate MAC addresses can access the network.

Configuration Example

Enabling WLAN-based MAB

Scenario **Figure 4-6**	

Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable WLAN-based MAB on the NAS. NAS configurations are as follows. For detailed configuration on the RADIUS server, see the *Configuring RADIUS*.
	`ruijie# configure terminal` `ruijie (config)# aaa new-model` `ruijie (config)# radius-server host 192.168.32.120` `ruijie (config)# radius-server key ruijie` `ruijie(config)#wlansec 1` `ruijie(config-wlansec)#dot1x-mab`
Verification	Check whether authentication is proper and network access behaviors change after authentication. ● The account is successfully created, such as **username: 0023aeaa4286,password: 0023aeaa4286**. ● The user fails to ping 192.168.32.120 before authentication. ● The user connects to the NAS, the authentication succeeds, and the user can successfully ping 192.168.32.120. ● Information of the authenticated user is displayed. `ruijie# show dot1x summary` `ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time` `--------- ---------- -------------- --------- ---- --------------- ------------- ---------- --------- ------------------` `16778217 0023aea... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s`

Common Errors

- The MAC account format is incorrect on the authentication server.

4.4.4 Configuring MAB Auto Authentication

Configuration Effect

- When a STA accesses the network for the first time, Web authentication is performed. When the STA is disconnected from and then reconnects to the network, authentication is not required.

Notes

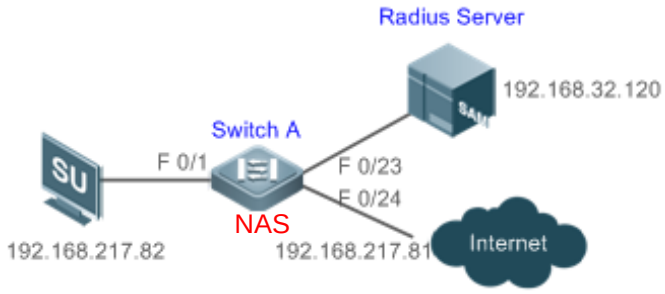
- Wireless MAB authentication is triggered by a STA advertisement. If a STA is already online, MAB authentication will not be triggered again. MAB authentication is triggered only after the STA is disconnected from and then reconnects to the network.
- When a STA accesses the network for the second time, a dialog box may be displayed for MAB authentication. When the STA accesses the network for the third time, the dialog box will not be displayed.
- If MAB authentication fails, a dialog box is displayed for Web authentication when the STA accesses the network next time.

Configuration Steps

For details about Web authentication configuration, see the Web authentication configuration document. For details about MAB authentication configuration, see section “Configuring MAB”.

Configuration Example

Configuring MAB Auto Authentication

Scenario **Figure 4-7**	
Configuration Steps	● Register the IP address of the NAS on the RADIUS server and configure the communication key between the NAS and the RADIUS server. ● Create an account on the RADIUS server and bind it with a MAC address for imperceptible authentication. ● Enable AAA on the NAS. ● Configure RADIUS parameters on the NAS. ● Enable 802.1X authentication and MAB authentication on an interface of the NAS. ● Enable second-generation (or first-generation/embedded) Web authentication on an interface of the NAS and configure the Web authentication template globally. The following describes the NAS configurations. For detailed configuration on the RADIUS server, see the related configuration guide (The following describes configuration on the switch, which is similar to that on the AC/AP, except that the configuration on the switch is performed in interface configuration mode instead of WLAN RSNA configuration mode.)
	`ruijie#configure terminal` `ruijie (config)#aaa new-model`

	ruijie (config)#aaa authentication web-auth default group radius ruijie (config)#aaa authentication dot1x default group radius ruijie (config)aaa accounting net-work default start-stop group radius ruijie (config)#radius-server host 192.168.32.120 ruijie (config)#radius-server key ruijie ruijie (config)#web-auth template eportalv2 ruijie (config-tmplt-v2)#ip 192.158.32.9 ruijie (config-tmplt-v2)#url http://192.168.32.9:8080/eportal/index.jsp ruijie (config-tmplt-v2)#exit ruijie (config)#interface FastEthernet 0/1 ruijie (config-if)#dot1x port-control auto ruijie (config-if)#dot1x mac-auth-bypass multi-user ruijie (config-if)#web-auth enable eportalv2
Verification	Check whether authentication is normal and network access behaviors change after authentication. ● The account is successfully created, for example, the username is 0023aeaa4286 and the password is 0023aeaa4286. ● The STA fails to ping 192.168.32.120 before authentication. ● The STA connects to the NAS, a page indicating the authentication succeeds is displayed, and the STA can successfully ping 192.168.32.120. ● The STA is disconnected from and then reconnects to the network and can successfully ping 192.168.32.120. ruijie#show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time --- --- --- --- --- --- --- --- --- --- 16778217 0023aea... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s

Common Errors

- The MAC account format is incorrect on the authentication server.

4.4.5 Configuring Extended Functions

Configuration Effect

- The multi-account function allows a user to switch its account upon re-authentication. In special scenarios such as Windows domain authentication, multiple authentications are required to access the domain and the user account changes during authentication. This function applies to these scenarios.
- 802.1X allows users to obtain IP addresses before accounting. In this manner, the IP address is carried during user accounting, meeting service requirements. After a user is authenticated and goes online, the NAS can obtain the IP

address of the user from the supplicant or through DHCP snooping, and then 802.1X server initiates an accounting request. To avoid the case in which the NAS does not initiate accounting for a long time due to failure to obtain the IP address of the authentication client, configure the IP detection timeout for this function. If the NAS does not obtain the IP address of the user within the configured time (5 minutes by default), it forces the user offline.

- 802.1X allows users to switch to the preset bypass WLAN when the RADIUS server is inaccessible. Survival WLANs are generally in OPEN mode and their services are unavailable by default. If 802.1X-based WLAN services are unavailable, enable this WLAN and disable WLAN-based 802.1X authentication so that users can switch to the bypass WLAN to properly access the network.
- 802.1X can be used with Web authentication. If Web authentication is enabled on an 802.1X-enabled WLAN, users perform 802.1X authentication only for encryption purposes. To access the network, they should also perform Web authentication. In this case, all air interface data of users is encrypted, enhancing security of user data.
- 802.1X provides prompts on syslog printing of user online/offline. You can adjust the online/offline syslog printing rate based on the user authentication rate to prevent high CPU utilization due to frequent syslog printing for a large number of users going online/offline.
- In the WLAN-based 802.1X authentication scenario, the NAS sends the authentication server SNMP traps to notify the online/offline status of users.
- In the WLAN-based 802.1X authentication scenario, traffic monitoring can be enabled on a WLAN. That is, if the traffic of an authenticated user is lower than the configured threshold within the specified period, the user will be forced offline so that the authentication server can perform accounting in a timely manner.
- Some servers deliver the accounting update interval only upon users' first authentication attempts. After re-authentication, users still use the accounting update interval configured on the NAS instead of that configured on the authentication server. To ensure the NAS to send accounting update packets according to the accounting update interval configured on the authentication server, you can configure users to always follow the accounting update interval assigned by the authentication server upon the first authentication.
- Based on a real scenario, H3C devices are deployed and the MAB authentication server configures the user name in xx-xx-xx-xx-xx-xx format. However, the default MAB authentication user name format of Ruijie devices is xxxxxxxxxxxx. Therefore, a command needs to be added to control the user name format.
- Based on a real scenario, wireless terminals use static IP addresses and need to report the IP addresses to the server. In 802.1X authentication mode, the default IP address source is obtained by runing the **ip dhcp snooping** command. **stamg** needs to be added to advertise the static IP address source.

Notes

- The multi-account function must be disabled if accounting is enabled. Otherwise, accounting may be inaccurate.
- IP-based accounting is not required in two situations:
  - IPv4 addresses and Ruijie Supplicant are deployed. This function is not required because Ruijie Supplicant can upload the IPv4 addresses of users.
  - Static IP addresses are deployed.

- It is recommended that the SSID of the bypass WLAN be different from that of the 802.1X-based WLAN so that the bypass WLAN services can be intuitively reflected. Moreover, when the WLAN needs to be switched due to server inaccessibility, users can manually switch the SSID once. Since the supplicant generally has a memory of the SSID, the SSID can be switched automatically in the future.
- Since 802.1X users are only for encryption purposes, the authorization, e.g., ACL assignment and rate limit assignment, to 802.1X users will not take effect. However, users need to pass Web authentication and be authorized to access the network.

Configuration Steps

Enabling Multi-account Authentication with One MAC Address

- (Optional) Run the **dot1x multi-account enable** command to allow the same MAC address to be used by multiple accounts.
- Enable multi-account authentication with one MAC address after 802.1X authentication is enabled on the NAS.

Command	**dot1x multi-account enable**
Parameter Description	N/A
Defaults	Multi-account authentication is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when multi-account authentication is required in 802.1X authentication, e.g. in the case of Windows domain authentication. In this case, the authentication client can directly use a new account to initiate authentication while the previous account is still online. Multi-account authentication is disabled by default.

Configuring the Maximum Number of Authenticated Users on a Port

- (Optional) You can restrict the number of online users on a controlled port, including static users and dynamic users.
- Configure the maximum number of authenticated users on a port after 802.1X authentication is enabled on the NAS.

Command	**dot1x default-user-limit** *num*
Parameter Description	*num*: Indicates the maximum number of online users.
Defaults	There is no restriction on the number of users on a port by default.
Command Mode	Interface configuration mode, VxLAN mode
Usage Guide	Configure this command when there is a need to restrict the number of authenticated users on a port.

Enabling IP-triggered Accounting

- (Optional) If IP-triggered accounting is enabled, the NAS sends an accounting request to the authentication server after obtaining the IP address of the user.
- Enable IP-triggered accounting after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct enable**
Parameter Description	N/A
Defaults	IP-triggered accounting is disabled by default.
Command Mode	Global configuration mode
Usage Guide	If both accounting and IP-triggered accounting are enabled, the NAS initiates accounting only after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address. If accounting is disabled but IP-triggered accounting is enabled, the NAS does not initiate accounting after obtaining the IP address of the authentication client, and forces the user offline if it fails to obtain the IP address within the timeout.

Configuring the Timeout of Obtaining IP Addresses After Authentication

- (Optional) Configure the timeout of obtaining IP addresses if IP-triggered accounting is enabled.
- Configure the IP address obtaining timeout after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct timeout** *time*
Parameter Description	*time:* Indicates the timeout in the unit of minutes.
Defaults	The default value is 5 minutes.
Command Mode	Global configuration mode
Usage Guide	It is recommended to use the default value. Configure this command when there is a need to change the IP address obtaining timeout after users pass authentication.

Configuring the Bypass WLAN for the RADIUS Server

- Optional.
- Enable bypass WLAN for the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**dot1x event server-invalid action bypass-wlan** *wlan_id*
Parameter Description	*wlan_id:* Indicates the bypass WLAN.
Defaults	Bypass WLAN is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This command applies only to wireless devices. It is recommended to use the default value. Configure this command when there is a need to provide the corresponding WLAN in the case of server inaccessibility.

Configuring 802.1X Authentication for Encryption Only When802.1X and Web Authentication Are Both Enabled

- (Optional) If 802.1X and Web authentication is enabled meanwhile, 802.1X is used only for encryption.

- Enable this function after 802.1X authentication is enabled on the NAS.

Command	**dot1x encryption only**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	It is recommended to retain the default setting. This command applies only to wireless devices.

Limiting the Rate of Printing Online and Offline Logs

- (Optional) You can limit the syslog printing rate upon 802.1X users going online/offline.
- Enable the syslog printing rate limit after 802.1X authentication is enabled on the NAS.

Command	**dot1x logging rate-limit** *value*
Parameter Description	*value:* Indicates the syslog printing rate per second upon users going online/offline. The default value is 5 per second. 0 indicates no rate limit.
Defaults	The default value is 5 per second.
Command Mode	Global configuration mode
Usage Guide	Generally it is recommended to use the defaults. If a large number of users frequently go online/offline, reduce this rate. This command applies only to wireless devices.

Enabling SNMP Trap During Online and Offline

- (Optional) The **dot1x user-trap enable** command is used to control whether to send traps to the SNMP server when 802.1X users go online or offline.
- Enable SNMP trap after 802.1X authentication is enabled on the NAS.

Command	**dot1x user-trap enable**
Parameter Description	N/A
Defaults	SNMP trap is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This command applies only to wireless 802.1X authentication devices. Configure this command when the NAS should send online/offline traps to the SNMP server. You also need to enable trap on the SNMP server. For details, see the *Configuring SNMP*.

Enabling Traffic Detection

- (Optional) If traffic detection is enabled, 802.1X-authenticated users with traffic lower than the threshold in the detection period will be kicked off to avoid incorrect accounting.
- Enable traffic detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x offline-detect {[interval** *val***] | [flow** *num***]}**
Parameter Description	*val*: Indicates the detection period. The default value is 8 hours. *num*: Indicates the traffic threshold. The default value is 0 KB.
Defaults	By default, traffic detection is enabled on the AC but disabled on the APs.
Command Mode	WLAN security configuration mode
Usage Guide	This command applies only to wireless 802.1X authentication devices. Configure this command when the NAS needs to detect STAs offline in a timely manner to prevent incorrect accounting.

Using the Accounting Update Interval Delivered by the Server Upon the First Authentication

- (Optional) If this function is enabled, online users always use the accounting update interval assigned by the authentication server upon the first authentication, instead of the accounting update interval configured on the NAS.

Command	**dot1x acct-update base-on first-time server**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Configure this command when the authentication server does not deliver the accounting update interval upon user re-authentication but the NAS must send accounting update packets according to the accounting update interval assigned by the authentication server upon the first authentication.

Configuring the Format of MAB Authentication Username

- (Optional) This function works only to MAB authentication users.

Command	**dot1x mab-username format with-dot | with-colon | with-hyphen**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The **dot1x mab-username format with-dot** command specifies the format of “xxxx.xxxx.xxxx”. The **dot1x mab-username format with-colon** command specifies the format of “xx:xx:xx:xx:xx:xx”. The **dot1x mab-username format with-hyphen** command specifies the format of “xx-xx-xx-xx-xx-xx”.

Obtains Static IP Addresses

- (Optional) This function works to both 802.1X and MAB authentication users.

Command	dot1x get-static-ip enable
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable this function when a static IP address applied on a wireless device needs to be uploaded to the server. The static IP address is uploaded to the server via an accounting packet. And no terminal ID is containd when a static IP address is used.

4.5 Monitoring

Clearing

Authentication user information can be cleared after 802.1X is disabled.

Description	Command
Clears 802.1X user information.	**no do1x port-control auto**
Clears 802.1X user information.	**clear dot1x user**
Restores the default 802.1X configuration.	**dot1x default**

Notes

- The **dot1x default** command is used to restore global configurations.

Description	Command
Restore the default value of status machine timeout duration.	**dot1x timeout quiet-period** **dot1x timeout server-timeout** **dot1x timeout supp-timeout** **dot1x timeout tx-period**
Restore default values of configurations related to re-authentication.	**dot1x re-authentication** **dot1x timeout re-authperiod** **dot1x reauth-max**
Restore default values of configurations related to proactive requests.	**dot1x auto-req** **dot1x auto-req user-detect** **dot1x auto-req req-interval** **dot1x auto-req packet-num**
Restores the default value of the number of retransmission times.	**dot1x mac-req**

Restores the default value of the authentication mode.	**dot1x auth-mode**
Restore the default values of configurations related to client probing.	**dot1x client-probe enable** **dot1x probe-timer alive** **dot1x probe-timer interval**
Restores the default value of the function of supporting only the private client.	**dot1x private-supplicant-only**
Restores the default value of the pseudo source MAC address function.	**dot1x pseudo source-mac**
Restores the default value of the number of VLAN redirection times upon authentication failures.	**dot1x auth-fail max-attempt**
Restores the default value of the function of one MAC address for multiple accounts.	**dot1x multiaccount enable**
Restores the default value of the dot1x redirection function.	**dot1x redirect**
Restores the default value of the silent timeout duration.	**dot1x multi-mab quiet-period**
Restore the default values of functions related to accounting after obtaining the IP address.	**dot1x valid-ip-acct enable** **dot1x valid-ip-acct timeout**

Displaying

Description	Command
Displays the parameters and status of the RADIUS server.	**show radius server**
Displays 802.1X status and parameters.	**show dot1x**
Displays the active authentication status.	**show dot1x auto-req**
Displays the port control status.	**show dot1x port-control**
Displays the status and parameters of host probe.	**show dot1x probe-timer**
Displays of the information of authenticated users.	**show dot1x summary**
Displays the AP-based 802.1X authentication summary.	**show dot1x summary by-ap**

Displays the AP-group-based 802.1X authentication summary.	**show dot1x summary by-ap-group**
Displays the maximum times of EAP-Request/Challenge packet retransmission.	**show dot1x max-req**
Displays the information of controlled ports.	**show dot1x port-control**
Displays the re-authentication status.	**show dot1x re-authentication**
Displays the maximum times of EAP-Request/Identity packet retransmission.	**show dot1x reauth-max**
Displays the quiet period after authentication fails.	**show dot1x timeout quiet-period**
Displays the re-authentication interval.	**show dot1x timeout re-authperiod**
Displays the authentication server timeout.	**show dot1x timeout server-timeou**t
Displays the supplicant timeout.	**show dot1x timeout supptimeout**
Displays the interval of EAP-Request/Identity packet retransmission.	**show dot1x timeout tx-period**
Displays user information based on the user ID.	**show dot1x user id**
Displays user information based on the MAC address.	**show dot1x user mac**
Displays user information based on the user name.	**show dot1x user name**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs AAA. (For details, see the *Configuring AAA*.)	**debug aaa**
Debugs RADIUS. (For details, see the *Configuring RADIUS*.)	**debug radius**
Debugs 802.1X events.	**debug dot1x event**
Debugs 802.1X packets.	**debug dot1x packet**
Debugs 802.1X state machine (STM).	**debug dot1x stm**

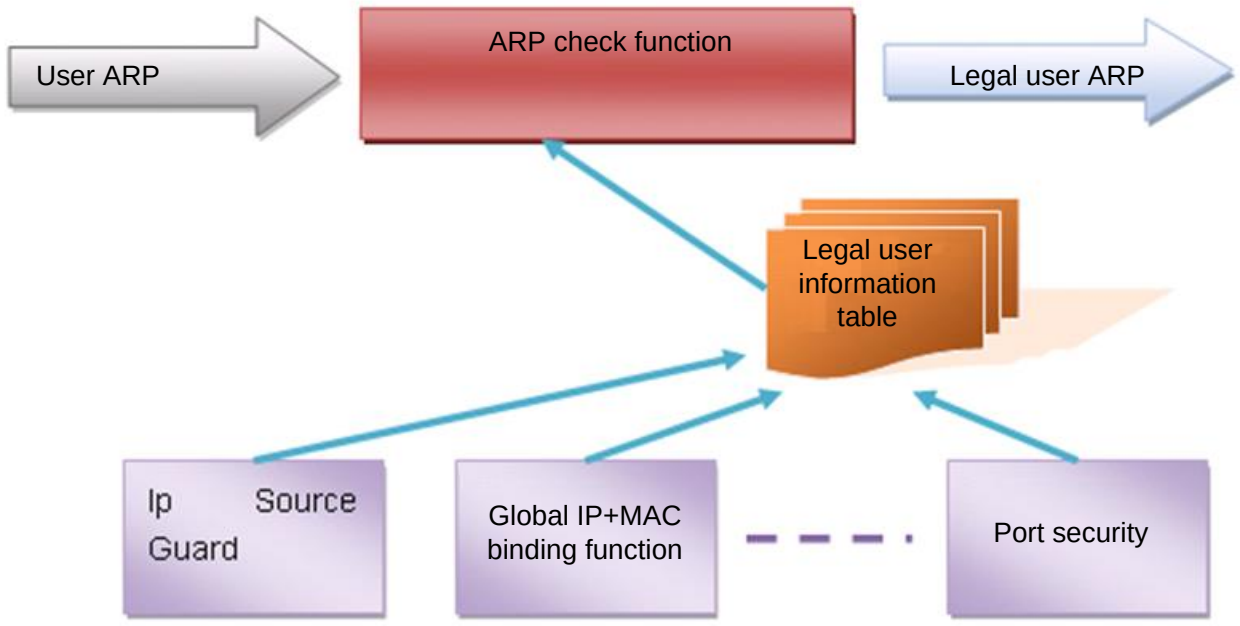
Debugs 802.1X internal communication.	**debug dot1x com**
Debugs 802.1X errors.	**debug dot1x error**

5 Configuring ARP Check

5.1 Overview

The Address Resolution Protocol (ARP) packet check filters all ARP packets under ports (including wired layer-2 switching ports, layer-2 aggregate ports (APs), and layer-2 encapsulation sub-interfaces, as well as WLAN interfaces) and discards illegal ARP packets, so as to effectively prevent ARP deception via networks and to promote network stability. On devices supporting ARP check, illegal ARP packets in networks will be ignored according to the legal user information (IP-based or IP-MAC based) generated by security application modules such as IP Source Guard, global IP+MAC binding, 802.1X authentication, GSN binding, Web authentication and port security.

Figure 5-1



The above figure shows that security modules generate legal user information (IP-based or IP-MAC based). ARP Check uses the information to detect whether the Sender IP fields or the <Sender IP, Sender MAC>fields in all ARP packets at ports matches those in the list of legal user information. If not, all unlisted ARP packets will be discarded.

Protocols and Standards

- RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

5.2 Applications

Application	Description

Filtering ARP packets in Networks	Illegal users in networks launch attacks using forged ARP packets.

5.2.1 Filtering ARP Packets in Networks

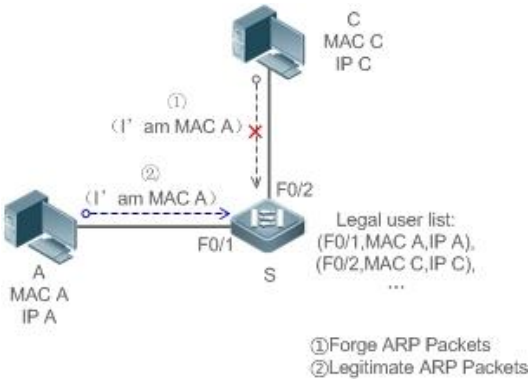
Scenario

Check ARP packets from distrusted ports and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

For example, in the following figure, the ARP packets sent by DHCP clients are checked.

- The ports receiving ARP packets, the source MAC addresses of ARP packets, and the source IP addresses of ARP packets shall be consistent with the snooped DHCP-assigned records.

Figure 5-2



Remarks:	S is an access device. A and C are user PCs.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all the downlink ports on S as DHCP distrusted ports.
- Enable IP Source Guard and ARP Check on all distrusted ports on S to realize ARP packet filtration.

5.3 Features

Basic Concepts

↘ Compatible Security Modules

Presently, the ARP Check supports the following security modules.

- IP-based: IP-based mode: port security, and static configuration of IP Source Guard.
- IP-MAC based: IP-MAC based mode: port security, global IP+MAC binding, 802.1X authorization, IP Source Guard, GSN binding, and Web authentication.

Two Modes of APR Check

The ARP Check has two modes: Enabled and Disabled. The default is Enabled.

17. Enabled Mode

Through ARP Check, ARP packets are detected based on the IP/IP-MAC based binding information provided by the following modules.

- Global IP-MAC binding
- 802.1X authorization
- IP Source Guard
- GSN binding
- Port security
- Web authentication
- Port security IP+MAC binding or IP binding

When only ARP Check is enabled on a port, the device allows all packets to pass. But if both ARP check and the above-mentioned modules are enabled, but user information cannot be generated, and thereby all ARP packets from this port will be discarded.

When the ARP Check and VRRP functions are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, the physical IP address and VRRP IP address need to be permitted to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

18. Disabled Mode

ARP packets on a port are not checked.

Overview

Feature	Description
Filtering ARP Packets	Check the source IP and source MAC addresses of ARP packets to filter out illegal ARP packets.

5.3.1 Filtering ARP Packets

Enable ARP Check on specified ports to realize filtration of illegal ARP packets.

Working Principle

A device matches the source IP and source MAC addresses of the ARP packets received at its ports with the legal user information of the device. With successful matching, packets will be transferred, or otherwise they will be discarded.

Related Configuration

Enabling ARP Check on Ports

By default, the ARP Check is disabled on ports.

Use the **arp-check** command to enable ARP Check.

Unless otherwise noted, this function is usually configured on the ports of access devices.

5.4 Configuration

Configuration	Description and Command	
Configuring ARP Check	(Mandatory) It is used to enable APR Check.	
	arp-check	Enables ARP Check.

5.4.1 Configuring ARP Check

Configuration Effect

- Illegal ARP packets are filtered out.

Notes

- When ARP Check is enabled, the number of policies or users of related security applications may decrease.
- ARP Check cannot be configured on mirrored destination ports.
- ARP Check cannot be configured on the trusted ports of DHCP Snooping.
- ARP Check cannot be configured on global IP+MAC exclude ports.
- ARP Check can be enabled only on wired switching ports, layer-2 APs, layer-2 encapsulation sub-interfaces, as well as WLAN interfaces. Enable ARP check for the wired in interface configuration mode, while for the wireless in WLAN security configuration mode.
- For fit APs in wired access mode, ARP Check needs to be enabled in ap-config all mode.

Configuration Steps

↘ Enabling ARP Check

- (Mandatory) The function is disabled by default. To use the ARP Check function, an administrator needs to run a command to enable it.

Verification

- Use the **show run** command to display the system configuration.
- Use the **show interface** { *interface-type interface-number* } **arp-check list** command to display filtering entries.

Related Commands

↘ Enabling ARP Check

Command	**arp-check**
Parameter Description	N/A
Command	Interface configuration mode, WLAN security configuration mode, or WLAN ap-config all configuration mode
Usage Guide	Generate ARP filtration information according to the legal user information of security application modules to filter out illegal ARP packets in networks. When the ARP Check function is enabled in WLAN ap-config all mode, the function is enabled on wired ports of all APs.

Configuration Example

The following configuration example introduces only ARP Check related configurations.

Enabling ARP Check on ports

Configuration Steps	● Enable ARP Check. Restricted ARP packets must conform to entries of IP Source Guard, port security, or global IP+MAC binding.

	Ruijie# configure terminal Ruijie(config)#address-bind 192.168.1.3 00D0.F800.0003 Ruijie(config)#address-bind install Ruijie(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1 Ruijie(config)# interface GigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)#arp-check Ruijie(config-if-GigabitEthernet 0/1)#ip verify source port-security Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1 192.168.1.1 Ruijie(config-if-GigabitEthernet 0/1)#exit Ruijie(config)#interface gigabitEthernet 0/4 Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5 Ruijie(config-if-GigabitEthernet 0/4)#arp-check Ruijie(config-if-GigabitEthernet 0/4)#exit Ruijie(config)#interface gigabitEthernet 0/5 Ruijie(config-if-GigabitEthernet 0/5)#arp-check Ruijie(config-if-GigabitEthernet 0/5)#end Ruijie# configure terminal Ruijie(config)#wlan-config 1 RUIJIE-SSID Ruijie(config-wlan)#end Ruijie#conf Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#wlansec 1 Ruijie(config-wlansec)# ip verify source port-security Ruijie(config-wlansec)#arp-check Ruijie(config-wlansec)#end Ruijie#conf Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1

Verification	Use the **show interfaces arp-check list** command to display the effective ARP Check list for interfaces.

```
Ruijie# show interfaces arp-check list

INTERFACE               SENDER MAC          SENDER IP           POLICY SOURCE
----------------------- ------------------- ------------------- -------------------
GigabitEthernet 0/1     00d0.f800.0003      192.168.1.3         address-bind
GigabitEthernet 0/1     00d0.f800.0001      192.168.1.1         port-security
GigabitEthernet 0/1     00d0.f800.0002      192.168.1.4         DHCP snooping
GigabitEthernet 0/4     00d0.f800.0003      192.168.1.3         address-bind
GigabitEthernet 0/4                         192.168.1.5         port-security
GigabitEthernet 0/5     00d0.f800.0003      192.168.1.3         address-bind

Ruijie# show wlan arp-check list

INTERFACE               SENDER MAC          SENDER IP           POLICY SOURCE
----------------------- ------------------- ------------------- -------------------
Wlan 1                  0026.c79f.6e4c      172.168.131.1       DHCP snooping
```

Common Errors

- If ARP packets at a port need to be checked but APR-Check is disabled, then APR-Check will not be effective.

5.5 Monitoring

Displaying

Description	Command
Displays the effective ARP Check list based on ports.	**show interface** [*interface-type interface-number*] **arp-checklist**
Displays the effective ARP Check list based on WLAN.	**show wlan** [*wlan-id*] **arp-checklist**

6 Configuring Gateway-targeted ARP Spoofing Prevention

6.1 Overview

Gateway-targeted Address Resolution Protocol (ARP) spoofing prevention effectively prevents gateway-targeted ARP spoofing by checking on the logical port whether the source IP addresses of ARP packets (Sender IP fields of ARP packets) are the self-configured gateway IP addresses.

Protocols and Standards

RFC 826: Ethernet Address Resolution Protocol

6.2 Applications

N/A

6.3 Features

Basic Concepts

ARP

ARP is a TCP/IP protocol that obtains physical addresses according to IP addresses. Its function is as follows: The host broadcasts ARP requests to all hosts on the network and receives the returned packets to determine physical addresses of the target IP addresses, and saves the IP addresses and hardware addresses in the local ARP cache, which can be directly queried in response to future requests. On the same network, all the hosts using the ARP are considered as mutually trustful to each other. Each host on the network can independently send ARP response packets; the other hosts receive the response packets and record them in the local ARP cache without detecting their authenticity. In this way, attackers can send forged ARP response packets to target hosts so that the messages sent from these hosts cannot reach the proper host or reach a wrong host, thereby causing ARP spoofing.

Gateway-targeted ARP Spoofing

When User A sends an ARP packet requesting the media access control (MAC) address of a gateway, User B on the same VLAN also receives this packet, and User B can send an ARP response packet, passing off the gateway IP address as the source IP address of the packet, and User B's MAC address as the source MAC address. This is called gateway-targeted ARP spoofing. After receiving the ARP response, User A regards User B's machine as the gateway, so all the packets sent from User A to the gateway during communication will be sent to User B. In this way, User A's communications are intercepted, thereby causing ARP spoofing.

Overview

Feature	Description
Gateway-targeted ARP Spoofing Prevention	Blocks ARP spoofing packets with forged gateway address and intranet server IP addresses to ensure that users can access the Internet.

6.3.1 Gateway-targeted ARP Spoofing Prevention

Working Principle

Gateway-targeted Spoofing Prevention

Gateway-targeted ARP spoofing prevention effectively prevents ARP spoofing aimed at gateways by checking on the logical port whether the source IP addresses of ARP packets are the self-configured gateway IP addresses. If an ARP packet uses the gateway address as the source IP address, the packet will be discarded to prevent users from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the devices connected to the switch can send ARP packets, and the ARP response packets sent from the other PCs which pass for the gateway are filtered by the switch.

Related Configuration

Configuring Gateway-targeted Spoofing Prevention Addresses

- By default, no gateway-targeted ARP spoofing prevention address is configured.
- Run the **anti-arp-spoofing ip** command to configure the gateway-targeted ARP spoofing prevention addresses.

6.4 Configuration

Configuration	Description and Command	
Configuring Gateway-targeted Spoofing Prevention	Optional.	
	anti-arp-spoofing ip	Configures gateway-targeted ARP spoofing prevention on the logical port and specifies the gateway IP address.

6.4.1 Configuring Gateway-targeted Spoofing Prevention

Configuration Effect

Enable gateway-targeted ARP spoofing prevention.

Configuration Steps

Configuring Gateway-targeted Spoofing Prevention

- Gateway-targeted ARP spoofing prevention is mandatory. It must be enabled.

Verification

- Run the **show run** command to check configuration.
- Run the **show anti-arp-spoofing** command to display all data on gateway-targeted ARP spoofing prevention.

Related Commands

Configuring Gateway-targeted Spoofing Prevention

Command	**anti-arp-spoofing ip** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of the gateway.
Command Mode	wireless security configuration mode
Usage Guide	

Configuration Example

N/A

6.5 Monitoring

Displaying

Description	Command
Displays all data on gateway-targeted ARP spoofing prevention.	**show anti-arp-spoofing**

7 Configuring Global IP-MAC Binding

7.1 Overview

Enable the global IP-MAC binding function manually to verify the input packets. If a specified IP address is bound with a MAC address, the device receives only the IP packets containing matched IP address and MAC address. The other packets are discarded.

The address bounding feature is used to verify the input packets. Note that the address binding feature takes precedence over the 802.1X authentication, port security, and access control list (ACL).

7.2 Applications

N/A

7.3 Features

Basic Concepts

↘ IPv6 Address Binding Mode

IPv6 address binding modes include Compatible, Loose, and Strict. The default mode is Strict. If IPv4-MAC binding is not configured, the IPv6 address binding mode does not take effect, and all IPv4 and IPv6 packets are allowed to pass through. If IPv4-MAC binding is configured, the IPv6 address binding mode takes effect, and the device forwards IPv4 and IPv6 packets based on the forwarding rules described in the following table:

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the global IPv4-MAC binding are forwarded.	Packets matching the global IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)
Loose	Packets matching the global IPv4-MAC binding are forwarded.	If IPv6+MAC address binding is configured, packets matching the IPv6-MAC binding are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.) If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.

Compatible	Packets matching the global IPv4-MAC binding are forwarded.	If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded. Packets matching the global IPv6-MAC binding conditions are forwarded. (The binding is generated by other access security functions, such as port security and IPv6 Source Guard.)

Overview

Feature	Description
Configuring the IPv6 Address Binding Mode	Change the IPv6 packet forwarding rules.

7.3.1 Configuring the IPv6 Address Binding Mode

Working Principle

After the global IPv4-MAC binding is configured and enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 binding modes include Compatible, Loose, and Strict.

Related Configuration

Configuring the IPv6 Address Binding Mode

By default, the IPv6 address binding mode is Strict.

Run the **address-bind ipv6-mode** command to specify an IPv6 address binding mode.

7.4 Configuration

Configuration	Description and Command	
Configuring the IPv6 Address Binding Mode	(Optional) It is used to configure the IPv6 address binding mode.	
	address-bind ipv6-mode	Configures the IPv6 address binding mode.

7.4.1 Configuring the IPv6 Address Binding Mode

Configuration Effect

- Change the IPv6 address binding mode so as to change the forwarding rules for IPv6 packets.

Configuration Steps

Configuring the IPv6 Address Binding Mode

- (Optional) Perform this configuration when you want to change the forwarding rules for IPv6 packets.

Verification

- Run the **show run** command to check whether the configuration takes effect.

Related Commands

Configuring the IPv6 Address Binding Mode

Command	**address-bind ipv6-mode** { **compatible | loose | strict** }
Parameter Description	**compatible**: Indicates the Compatible mode. **loose**: Indicates the Loose mode. **strict**: Indicates the strict mode.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Configuring the IPv6 Address Binding Mode

Configuration Steps	• Configure a global IP-MAC binding. • Enable the address binding function. • Set the IPv6 address binding mode to Compatible.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001 Ruijie(config)# address-bind install Ruijie(config)# address-bind ipv6-mode compatible
Verification	Run the **show run** command to display the configuration on the device.

7.5 Monitoring

Displaying

N/A

8 Configuring DHCP Snooping

8.1 Overview

DHCP Snooping: DHCP Snooping snoops DHCP interactive packets between clients and servers to record and monitor users' IP addresses and filter out illegal DHCP packets, including client request packets and server response packets. The legal user database generated from DHCP Snooping records may serve security applications like IP Source Guard.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

8.2 Applications

Application	Description
Guarding against DHCP service spoofing	In a network with multiple DHCP servers, DHCP clients are allowed to obtain network configurations only from legal DHCP servers.
Guarding against DHCP packet flooding	Malicious network users may frequently send DHCP request packets.
Guarding against forged DHCP packets	Malicious network users may send forged DHCP request packets, for example, DHCP-RELEASE packets.
Guarding against IP/MAC spoofing	Malicious network users may send forged IP packets, for example, tampered source address fields of packets.
Preventing Lease of IP Addresses	Network users may lease IP addresses rather than obtaining them from a DHCP server.
Detecting ARP attack	Malicious users forge ARP response packets to intercept packets during normal users' communication.

8.2.1 Guarding Against DHCP Service Spoofing

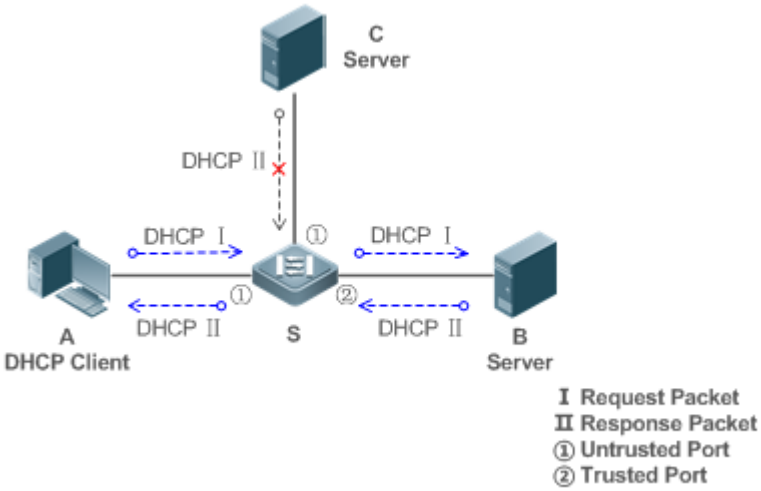
Scenario

Multiple DHCP servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

Take the following figure as an example. The DHCP client can only communicate with trusted DHCP servers.

- Request packets from the DHCP client can be transmitted only to trusted DHCP servers.
- Only the response packets from trusted DHCP servers can be transmitted to the client.

Figure 8-1



Remarks:	S is an access device. A is a user PC. B is a DHCP server within the controlled area. C is a DHCP server out of the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP packet monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.

8.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients in a network may send high-rate DHCP packets. As a result, legitimate users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the DHCP Snooping rate limit function for DHCP packets, a DHCP client can only send DHCP request packets at a rate below the limit.

- The request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Enable DHCP Snooping correlation with ARP, and delete the non-existing entries.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Limit the rates of DHCP packets from the untrusted ports.

- Enable DHCP Snooping correlation with ARP, and detect whether the user is online.

8.2.3 Guarding Against Forged DHCP Packets

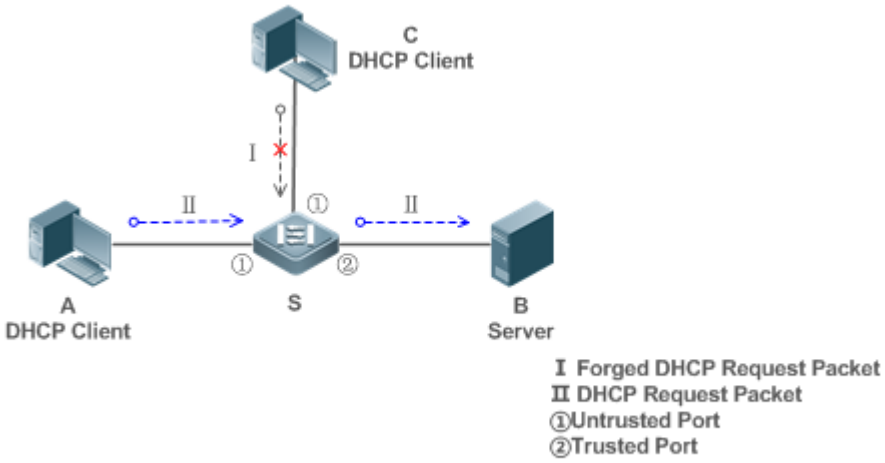
Scenario

Potential malicious clients in a network may forge DHCP request packets, consuming applicable IP addresses from the servers and probably preempting legal users' IP addresses. Therefore, it is necessary to filter out illegal DHCP packets.

For example, as shown in the figure below, the DHCP request packets sent from DHCP clients will be checked.

- The source MAC address fields of the request packets from DHCP clients must match the **chaddr** fields of DHCP packets.
- The Release packets and Decline packets from clients must match the entries in the DHCP Snooping binding database.

Figure 8-2



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set the port on S connecting to B as trusted to transfer response packets.
- Set the rest of ports on S as untrusted to filter response packets.
- Enable DHCP Snooping Source MAC Verification on untrusted ports of S to filter out illegal packets.

8.2.4 Guarding Against IP/MAC Spoofing

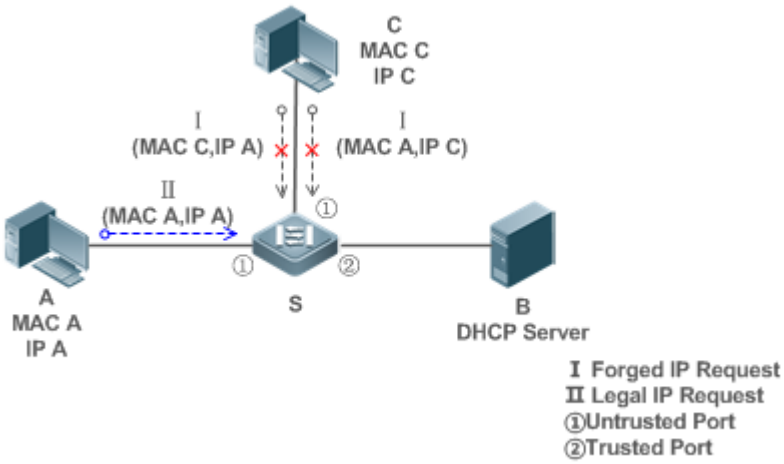
Scenario

Check IP packets from untrusted ports to filter out forged IP packets based on IP or IP-MAC fields.

For example, in the following figure, the IP packets sent by DHCP clients are validated.

- The source IP address fields of IP packets must match the IP addresses assigned by DHCP.
- The source MAC address fields of layer-2 packets must match the **chaddr** fields in DHCP request packets from clients.

Figure 8-3



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as DHCP Snooping untrusted.
- Enable IP Source Guard on S to filter IP packets.
- Enable IP Source Guard in IP-MAC based mode to check the source MAC and IP address fields of IP packets.

8.2.5 Preventing Lease of IP Addresses

Scenario

Validate the source addresses of IP packets from untrusted ports compared with DHCP-assigned addresses.

If the source addresses, connected ports, and layer-2 source MAC addresses of ports in IP packets do not match the assignments of the DHCP server, such packets will be discarded.

The networking topology scenario is the same as that shown in the previous figure.

Deployment

- The same as that in the section "Guarding Against IP/MAC Spoofing".

8.2.6 Detecting ARP Attacks

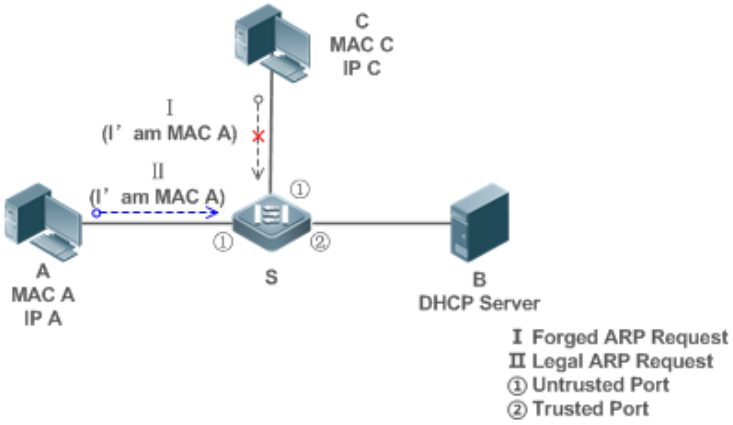
Scenario

Check the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

For example, in the following figure, the ARP packets sent from DHCP clients will be checked.

- The ports receiving ARP packets, the layer-2 MAC addresses, and the source MAC addresses of ARP packets senders shall be consistent with the DHCP Snooping histories.

Figure 8-4



Remarks:	S is an access device. A and C are user PCs. B is a DHCP server within the controlled area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on the S as untrusted.
- Enable IP Source Guard and ARP Check on all the untrusted ports on S to realize ARP packet filtering.

All the above security control functions are only effective to DHCP Snooping untrusted ports.

8.3 Features

Basic Concepts

DHCP Request Packets

Request packets are sent from a DHCP client to a DHCP server, including DHCP-DISCOVER packets, DHCP-REQUEST packets, DHCP-DECLINE packets, DHCP-RELEASE packets and DHCP-INFORM packets.

DHCP Response Packets

Response packets are sent from a DHCP server to a DHCP client, including DHCP-OFFER packets, DHCP-ACK packets and DHCP-NAK packets.

DHCP Snooping Trusted Ports

IP address request interaction is complete via broadcast. Therefore, illegal DHCP services will influence normal clients' acquisition of IP addresses and lead to service spoofing and stealing. To prevent illegal DHCP services, DHCP Snooping ports are divided into two types: trusted ports and untrusted ports. The access devices only transmit DHCP response packets received on trusted ports, while such packets from untrusted ports are discarded. In this way, we may configure the ports connected to a legal DHCP Server as trusted and the other ports as untrusted to shield illegal DHCP Servers.

On switches, all switching ports or layer-2 aggregate ports are defaulted as untrusted, while trusted ports can be specified. On wireless access points (APs), all the WLAN interfaces are untrusted and cannot be specified as trusted. In fat AP configuration mode, all the layer-2 switching ports and layer-2 encapsulation sub-interfaces are untrusted by default, and can be specified as trusted. In fit AP configuration mode, all the layer-2 switching ports are untrusted by default and can be specified as trusted, and all the layer-2 encapsulation sub-interfaces are trusted and cannot be specified as untrusted. On wireless access controllers (ACs), all WLAN interfaces are untrusted ports and cannot be specified as trusted, and all the switching ports and layer-2 aggregate ports are untrusted ports by default and can be specified as trusted.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, we can enable DHCP Snooping packet suppression on its untrusted ports.

VLAN-based DHCP Snooping

DHCP Snooping can work on a VLAN basis. By default, when DHCP Snooping is enabled, it is effective to all the VLANs of the current client. Specify VLANs help control the effective range of DHCP Snooping flexibly.

DHCP Snooping Binding Database

In a DHCP network, clients may set static IP addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legal clients with IP addresses assigned by the DHCP server may fail to use the network normally due to address conflict. Through snooping packets between clients and servers, DHCP Snooping summarizes the user entries including IP addresses, MAC address, VLAN ID (VID), ports and lease time to build the DHCP

Snooping binding database. Combined with ARP detection and ARP check, DHCP Snooping controls the reliable assignment of IP addresses for legal clients.

DHCP Snooping Rate Limit

DHCP Snooping rate limit function can be configured through the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see the *Configuring NFPP*.

DHCP Option82

DHCP Option82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option82. Option82 is developed to enhance the security of DHCP servers and improve the strategies of IP address assignment. The option is often configured for the DHCP relay services of a network access device like DHCP Relay and DHCP Snooping. This option is transparent to DHCP clients, and DHCP relay components realize the addition and deduction of the option.

Illegal DHCP Packets

Through DHCP Snooping, validation is performed on the DHCP packets passing through a client. Illegal DHCP packets are discarded, user information is recorded into the DHCP Snooping binding database for further applications (for example, ARP detection). The following types of packets are considered illegal DHCP packets.

- The DHCP response packets received on untrusted ports, including DHCP-ACK, DHCP-NACK and DHCP-OFFER packets
- The DHCP request packets carrying gateway information **giaddr**, which are received on untrusted ports
- When MAC verification is enabled, packets with source MAC addresses different with the value of the **chaddr** field in DHCP packets
- DHCP-RELEASE packets with the entry in the DHCP Snooping binding database Snooping while with untrusted ports inconsistent with settings in this binding database
- DHCP packets in wrong formats, or incomplete

Overview

Feature	Description
Filtering DHCP packets	Perform legality check on DHCP packets and discard illegal packets (see the previous section for the introduction of illegal packets). Transfer requests packets received on trusted ports only.
Building the DHCP Snooping binding database	Snoop the interaction between DHCP clients and the server, and generate the DHCP Snooping binding database to provide basis for other filtering modules.

8.3.1 Filtering DHCP Packets

Perform validation on DHCP packets from untrusted ports. Filter out the illegal packets as introduced in the previous section "Basic Concepts".

Working Principle

During snooping, check the receiving ports and the packet fields of packets to realize packet filtering, and modify the destination ports of packets to realize control of transmit range of the packets.

Checking Ports

In receipt of DHCP packets, a client first judges whether the packet receiving ports are DHCP Snooping trusted ports. If yes, legality check and binding entry addition are skipped, and packets are transferred directly. For not, both the check and addition are needed.

Checking Packet Encapsulation and Length

A client checks whether packets are UDP packets and whether the destination port is 67 or 68. Check whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of illegal packet introduced in the section "Basic Concepts", check the fields **giaddr** and **chaddr** in packets and then check whether the restrictive conditions for the type of the packet are met.

Related Configuration

Enabling Global DHCP Snooping

By default, DHCP Snooping is disabled.

It can be enabled on a device using the **ip dhcp snooping** command.

Global DHCP Snooping must be enabled before VLAN-based DHCP Snooping is applied.

Configuring VLAN-based DHCP Snooping

By default, when global DHCP Snooping is effective, DHCP Snooping is effective to all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP Snooping on specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN numbers.

Configuring DHCP Snooping Source MAC Verification

By default, the layer-2 MAC addresses of packets and the **chaddr** fields of DHCP packets are not verified.

When the **ip dhcp snooping verify mac-address** command is used, the source MAC addresses and the **chaddr** fields of the DHCP request packets sent from untrusted ports are verified. The DHCP request packets with different MAC addresses will be discarded.

8.3.2 Building the Binding Database

DHCP Snooping detects the interactive packets between DHCP clients and the DHCP server, and generate entries of the DHCP Snooping binding database according to the information of legal DHCP packets. All these legal entries are provided to other security modules of a client as the basis of filtering packets from network.

Working Principle

During snooping, the binding database is updated timely based on the types of DHCP packets.

Generating Binding Entries

When a DHCP-ACK packet on a trusted port is snooped, the client's IP address, MAC address, and lease time field are extracted together with the port ID (a wired interface index or a WLAN ID) and VLAN ID. Then, a binding entry of it is generated.

Deleting Binding Entries

When the recorded lease time of a binding entry is due, it will be deleted if a legal DHCP-RELEASE/DHCP-DECLINE packet sent by the client or a DHCP-NCK packet received on a trusted port is snooped, or the **clear** command is used.

Related Configuration

No configuration is needed except enabling DHCP Snooping.

8.4 Configuration

Configuration	Description and Command	
Configuring basic functions of DHCP Snooping	⚠ (Mandatory) It is used to enable DHCP Snooping.	
	ip dhcp snooping	Enables DHCP Snooping.
	ip dhcp snooping suppression	Enables DHCP Snooping packet suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP Snooping.
	ip dhcp snooping verify mac-address	Configures DHCP Snooping source MAC verification.
	ip dhcp snooping database write-delay	Writes the DHCP Snooping binding database to Flash periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP Snooping binding database to Flash manually.
	renew ip dhcp snooping database	Imports user information in the backup file to the DHCP Snooping Binding database.
	ip dhcp snooping trust	Configures DHCP Snooping trusted ports.
	ip dhcp snooping bootp	Enables BOOTP support.
	ip dhcp snooping check-giaddr	Enables DHCP Snooping to support the function of processing Relay requests.
	ip dhcp snooping clear-broadcast-flag	Enables the function of clearing the broadcast flag bit.
Configuring Option82	⚠ (Optional)It is used to optimize the address assignment by DHCP servers.	

	ip dhcp snooping Information option	Adds Option82 functions to DHCP request packets.
	ip dhcp snooping information option format remote-id	Configures the sub-potion **remote-id** of Option82 as a user-defined character string.
	ip dhcp snooping vlan information option format-type circuit-id string	Configures the sub-option **circuit-id** of Option82 as a user-defined character string.

8.4.1 Configuring Basic Features

Configuration Effect

- Enable DHCP Snooping.
- Generate the DHCP Snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out illegal DHCP packets.

Notes

- The ports on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP Snooping is effective on the wired switching ports, layer-2 aggregate ports, and layer-2 encapsulation sub-interfaces, as well as WLAN interfaces. The configuration can be implemented in interface configuration mode and WLAN security configuration mode.

Configuration Steps

↘ Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, the feature should be configured on access devices.

↘ Enabling or Disabling VLAN-based DHCP Snooping

- DHCP Snooping can be disabled if not necessary for some VLANs.
- Unless otherwise noted, the feature should be configured on access devices.

↘ Configuring DHCP Snooping Trusted Ports

- Mandatory.
- Configure the ports connecting a trusted DHCP server as trusted.

↘ Enabling DHCP Snooping Source MAC Validation

- This configuration is required if the **chaddr** fields of DHCP request packets match the layer-2 source MAC addresses of data packets.
- Unless otherwise noted, the feature should be enabled on all the untrusted ports of access devices.

Writing the DHCP Snooping Binding Database to Flash Periodically

- Enable this feature to timely save the DHCP Snooping binding database information in case that client reboot.
- STA information is not saved.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling BOOTP Support

- Optional
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping Correlation with ARP

- Optional.
- Unless otherwise noted, the feature should be configured on access devices.

Enabling DHCP Snooping to Process Relay Requests

- Optional.
- Unless otherwise noted, the feature should be enabled on access devices.

Enabling DHCP Snooping to Clear the Broadcast Flag Bit

- Optional.
- Unless otherwise noted, the feature should be enabled in large Layer-2 wireless scenarios.

Verification

Configure a client to obtain network configurations through the DHCP protocol.

- Check whether the DHCP Snooping Binding database is generated with entries on the client.

Related Commands

Enabling or Disabling DHCP Snooping

Command	[**no**] **ip dhcp snooping**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After global DHCP Snooping is enabled, you can check DHCP Snooping using the **show ip dhcp snooping** command.

Configuring VLAN-based DHCP Snooping

Command	[**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }
Parameter	*vlan-rng*: Indicates the range of VLANs

Description	*vlan-min*: The minimum VLAN ID *vlan-max*: The maximum VLAN ID
Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP Snooping on specified VLANs. This feature is available only after global DHCP Snooping is enabled.

Configuring DHCP Snooping Packet Suppression

Command	[**no**] **ip dhcp snooping suppression**
Parameter Description	**N/A**
Command Mode	Interface configuration mode/WLAN security configuration mode
Usage Guide	Use this command to reject all DHCP request packets at the port, that is, to forbid all users under the port to apply for addresses via DHCP.

Configuring DHCP Snooping Source MAC Verification

Command	[**no**] **ip dhcp snooping verify mac-address**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Through the source MAC address verification, the MAC addresses in link headers and the CLIENT MAC fields in the request packets sent by a DHCP CLIENT are checked for consistence. When the source MAC address verification fails, packets will be discarded.

Writing DHCP Snooping Database to Flash Periodically

Command	[**no**] **ip dhcp snooping database write-delay** [*time*]
Parameter Description	*time*: Indicates the interval between two times of writing the DHCP Snooping database to the Flash.
Command Mode	Global configuration mode
Usage Guide	Use this command to write the DHCP Snooping database to FLASH document. This can avoid binding information loss which requires re-obtaining IP addresses to resume communication after the device restarts.

Writing the DHCP Snooping Database to Flash Manually

Command	**ip dhcp snooping database write-to-flash**
Parameter Description	**N/A**

Command Mode	Global configuration mode
Usage Guide	Use this command to write the dynamic user information in the DHCP Snooping database in FLASH documents in real time. If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored from FLASH documents because of version differences between FLASH documents.

Importing Backep File Storage to the DHCP Snooping Binding Database

Command	**renew ip dhcp snooping database**
Parameter Description	**N/A**
Command Mode	Privileged configuration mode
Usage Guide	Use this command to import the information from backup file to the DHCP Snooping binding database.

Configuring DHCP Snooping Trusted Ports

Command	[**no**] **ip dhcp snooping trust**
Parameter Description	**N/A**
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure a port connected to a legal DHCP server as a trusted port. The DHCP response packets received by trusted ports are transferred, while those received by untrusted ports are discarded.

Enabling or Disabling BOOTP Support

Command	[**no**] **ip dhcp snooping bootp**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	Use this command to support the BOOPT protocol.

Enabling DHCP Snooping to Process Relay Requests

Command	[**no**] **ip dhcp snooping check-giaddr**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay

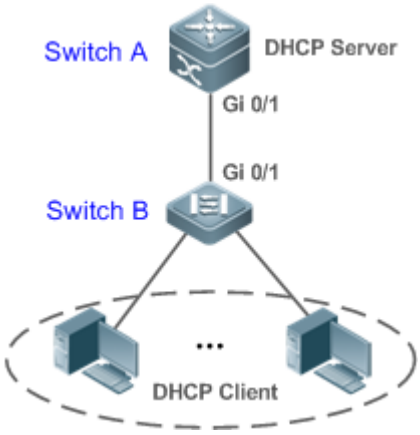
	requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

Enabling DHCP Snooping to Clear the Broadcast Flag Bit

Command	[**no**] **ip dhcp snooping clear-broadcast-flag**
Parameter Description	**N/A**
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, DHCP Snooping checks the broadcast flag bit for non-DHCP Relay requests. If the flag bit is 1, it clears the flag bit. When receiving responses, DHCP Snooping sets the flag bit to 1 and set Layer-2 and Layer-3 destination addresses as broadcast addresses.

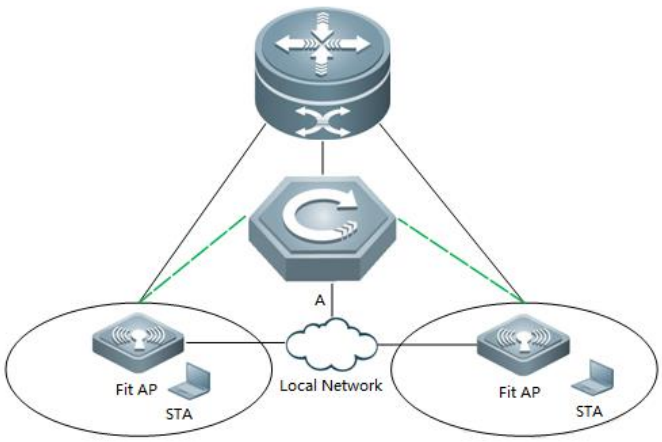
Configuration Example

DHCP Client Obtaining IP addresses Dynamically from a Legal DHCP Server

Scenario **Figure 8-5**	
Configuration Steps	● Enable DHCP Snooping on an access device (Switch B in this case). ● Configure the uplink port (port Gi 0/1 in this case) as a trusted port.
B	B#configure terminal Enter configuration commands, one per line. End with CNTL/Z. B(config)#ip dhcp snooping B(config)#interface gigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust B(config-if-GigabitEthernet 0/1)#end
Verification	Check the configuration on Switch B. ● Check whether DHCP Snooping is enabled, and whether the configured DHCP Snooping trusted port

	is uplink. ● Check the DHCP Snooping configuration on Switch B, and especially whether the trusted port is correct.
B	B#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : DISABLE DHCP Snooping Support BOOTP bind status : DISABLE Interface Trusted Rate limit (pps) ------------------------ ------- ---------------- GigabitEthernet 0/1 YES unlimited B#show ip dhcp snooping binding Total number of bindings: 1 MacAddress IpAddress Lease(sec) Type VLAN Interface ------------------ --------------- ------------ ------------- ----- -------------------- 0013.2049.9014 172.16.1.2 86207 DHCP-Snooping 1 GigabitEthernet 0/11

Configuring DHCP Snooping for Wireless Fit APs in Local Forwarding Scenarios

Scenario Figure 8-6	
Configuration Steps	● Configure DHCP Snooping basic functions on the wireless controller.
A	A# configure terminal A(config)# ip dhcp snooping A(config)# end

Verification	Check the DHCP Snooping configuration.
A	A#show ip dhcp snooping Switch DHCP snooping status : ENABLE DHCP snooping Verification of hwaddr status : DISABLE DHCP snooping database write-delay time : 0 seconds DHCP snooping option 82 status : DISABLE DHCP snooping Support bootp bind status : DISABLE Interface Trusted Rate limit (pps) ------------------------ ------- ---------------- Default No unlimited

Common Errors

- The uplink port is not configured as a DHCP trusted port.
- Another access security option is already configured for the uplink port, so that a DHCP trusted port cannot be configured.

8.4.2 Configuring Option82

Configuration Effect

- Enable a DHCP server to obtain more information and assign addresses better.
- The Option82 function is client-oblivious.

Notes

- The Opion82 functions for DHCP Snooping and DHCP Relay are mutually exclusive.

Configuration Steps

- To realize optimization of address allocation, implement the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP Snooping enabled.

Verification

Check whether the DHCP Snooping configuration options are configured successfully.

Related Commands

↘ Adding Option82 to DHCP Request Packets

Command	[**no**] **ip dhcp snooping information option** [**standard-format**]
Parameter Description	**standard-format**: Indicates a standard format of the Option82 options

Command Mode	Global configuration mode
Usage Guide	Use this command to add Option82 to DHCP request packets so that a DHCP server assigns addresses according to such information.

Configuring Sub-option remote-id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: Indicates the content of the extensible format, the Option82 option **remote-id**, is a user-defined character string **hostname**: Indicates the content of the extensible format, the Option82 option **remote-id**, is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuring Sub-Option circuit -id of Option82 as User-defined Character String

Command	[**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*
Parameter Description	*vlan-id*: Indicates the VLAN where a DHCP request packet is *ascii-string*: Indicates the user-defined string
Configuration mode	Interface configuration mode
Usage Guide	Use this command to configure the sub-option **circuit-id** of the Option82 as user-defined content, which is added to DHCP request packets. A DHCP server assigns addresses according to Option82 information.

Configuration Example

Configuring Option82 to DHCP Request Packets

Configuration Steps	● Configuring basic functions of DHCP Snooping. ● Configuring Option82.
B	`Ruijie# configure terminal` `Ruijie(config)# ip dhcp snooping information option` `Ruijie(config)# end`
Verification	Check the DHCP Snooping configuration.
B	`B#show ip dhcp snooping` `Switch DHCP Snooping  status                    :   ENABLE` `DHCP Snooping  Verification of hwaddr status    :   DISABLE` `DHCP Snooping database write-delay time         :   0 seconds` `DHCP Snooping option 82 status                 :   ENABLE` `DHCP Snooping Support bootp bind status         :   DISABLE` `Interface                      Trusted       Rate limit (pps)`

```
------------------------        -------        ----------------
GigabitEthernet 0/1             YES            unlimited
```

Common Errors

- N/A

8.5 Monitoring

Clearing

Running the clear commands may lose vital information and thus interrupt services.

Description	Command
Clears the DHCP Snooping binding database.	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-id*]

Displaying

Description	Command
Displays DHCP Snooping configuration.	**show ip dhcp snooping**
Displays the DHCP Snooping binding database.	**show ip dhcp snooping binding**

Debugging

System resources are occupied when debugging information is output. Disable the debugging switch immediately after use.

Description	Command
Debugs DHCP Snooping events.	**debug snooping ipv4 event**
Disables debugging DHCP Snooping events.	**no debug snooping ipv4 event**
Debugs DHCP Snooping packets.	**debug snooping ipv4 packet**
Disables debugging DHCP Snooping packets.	**no debug snooping ipv4 packet**

9 Configuring IP Source Guard

9.1 Overview

The IP Source Guard function realizes hardware-based IP packet filtering to ensure that only the users having their information in the binding database can access networks normally, preventing users from forging IP packets.

9.2 Applications

Application	Description
Guarding Against IP/MAC Spoofing Attack	In network environments, users set illegal IP addresses and malicious users launch attacks through forging IP packets.

9.2.1 Guarding Against IP/MAC Spoofing Attack

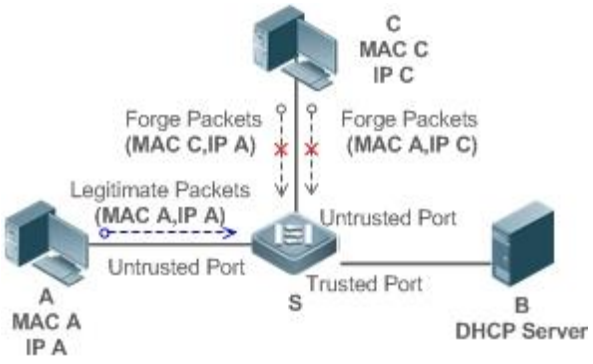
Scenario

Check the IP packets from DHCP untrusted ports. Forged IP packets will be filtered out based on the IP or IP-MAC field.

For example, in the following figure, the IP packets sent by DHCP clients are checked.

- The Source IP Address fields of IP packets should match DHCP-assigned IP addresses.
- The Source MAC Address fields of layer-2 packets should match the MAC addresses in DHCP request packets from clients.

Figure 9-1



Remarks:	S is a network access server (NAS). A and C are user PCs. B is a DHCP server within the control area.

Deployment

- Enable DHCP Snooping on S to realize DHCP monitoring.
- Set all downlink ports on S as DHCP untrusted ports.
- Enable IP Source Guard on S to realize IP packet filtering.
- Enable IP–MAC match mode for IP Source Guard on S, filtering IP packets based on IP and MAC addresses.

9.3 Features

Basic Concepts

Source IP Address

Indicate the source IP address field of an IP packet.

Source MAC Address

Indicate the source MAC address field of an IP packet.

IP-based Filtering

Indicate a policy of IP packet filtering, where only the source IP addresses of all IP packets (except DHCP packets) passing through a port are checked. It is the default filtering policy of IP Source Guard.

IP-MAC based Filtering

A policy of IP packet filtering, where both the source IP addresses and source MAC addresses of all IP packets are checked, and only those user packets with these IP addresses and MAC addresses existing in the binding database are permitted.

Address Binding Database

As the basis of security control of the IP Source Guard function, the data in the address binding database comes from two ways: the DHCP Snooping binding database and static configuration. When IP Source Guard is enabled, the data of the DHCP Snooping binding database is synchronized to the address binding database of IP Source Guard, so that IP packets can be filtered strictly through IP Source Guard on a device with DHCP Snooping enabled.

Excluded VLAN

By default, when IP Source Guard is enabled on a port, it is effective to all the VLANs under the port. Users may specify excluded VLANs, within which IP packets are not checked and filtered, which means that such IP packets are not controlled by IP Source Guard. At most 32 excluded VLANs can be specified for a port.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter the IP packets passing through ports by IP-based or IP-MAC based filtering.

9.3.1 Checking Source Address Fields of Packets

Filter the IP packets passing through ports based on source IP addresses or on both source IP addresses and source MAC addresses to prevent malicious attack by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to release such packets.

Working Principle

When IP Source Guard is enabled, the source addresses of packets passing through a port will be checked. The port can be a wired switching port, a layer-2 aggregate port (AP), or a layer-2 encapsulation sub-interface, or a WLAN interface. Such packets will pass the port only when the source address fields of the packets match the set of the address binding records generated by DHCP Snooping, or the static configuration set by the administrator. There are two matching modes as below.

IP-based Filtering

Packets are allowed to pass a port only if the source IP address fields of them belong to the address binding database.

IP-MAC Based Filtering

Packets are allowed to pass a port only when both the layer-2 source MAC addresses and layer-3 source IP addresses of them match an entry in the address binding database.

Specifying Excluded VLAN

Packets within such a VLAN are allowed to pass a port without check or filtering.

Related Configuration

Enabling IP Source Guard on a Port

By default, the IP Source Guard is disabled on ports.

It can be enabled using the **ip verify source** command.

Usually IP Source Guard needs to work with DHCP Snooping. Therefore, DHCP Snooping should also be enabled. DHCP Snooping can be enabled at any time on Ruijie devices, either before or after IP Source Guard is enabled.

Configuring a Static Binding

By default, legal users passing IP Source Guard check are all from the binding database of DHCP Snooping.

Bound users can be added using the **ip source binding** command.

Specifying an Excluded VLAN

By default, IP Source Guard is effective to all the VLANs under a port.

Excluded VLANs may be specified which are exempted from IP Source Guard using the **ip verify source exclude-vlan** command.

Excluded VLANs can be specified only after IP Source Guard is enabled on a port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on a port.

The above-mentioned port can be a wired switching port, a layer-2 AP port or a layer-2 encapsulation sub-interface, or a WLAN interface.

9.4 Configuration

Configuration	Description and Command	
Configuring IP Source Guard	(Mandatory) It is used to enable IP Source Guard.	
	ip verify source	Enables IP Source Guard on a port.
	ip source binding	Configures a static binding.
	Ip verify source exclude-vlan	Specifies an excluded VLAN for IP Source Guard.

9.4.1 Configuring IP Source Guard

Configuration Effect

- Check the source IP addresses of input IP packets.

Notes

- When IP Source Guard is enabled, IP packets forwarding may be affected. In general case, IP Source Guard is enabled together with DHCP Snooping.
- IP Source Guard cannot be configured on the trusted ports controlled by DHCP Snooping.
- IP Source Guard cannot be configured on the global IP+MAC exclusive ports.
- IP Source Guard can be configured and enabled only on wired switch ports, Layer-2 AP ports, Layer-2 encapsulation sub-ports and WLAN. In a wired access scenario, it is supposed to be configured in the interface configuration mode. In a wireless access scenario, it is supposed to be configured in the WLAN security configuration mode.
- For a Fit AP in a wired access scenario, IP Source Guard is configured and enabled in WLAN ap-config all configuration mode.

Configuration Steps

- Enable DHCP Snooping.
- Enable IP Source Guard.

Verification

Use the monitoring commands to display the address binding database of IP Source Guard.

Related Commands

Enabling IP Source Guard on a Port

Command	**ip verify source** [**port-security**]
Parameter Description	**port-security**: Enable IP-MAC based filtering.
Command	Interface configuration mode/WLAN security configuration mode/WLAN ap-config all configuration mode
Usage Guide	Detection of users based on IP address or both IP and MAC addresses can be realized by enabling IP Source Guard for a port. In the WLAN ap-config all configuration mode, once IP Source Guard is enabled, it works on all wired ports of the AP.

Configuring a Static Binding

Command	**ip source binding** *mac-address* **vlan** *vlan-id* **[***ip-address* **{ interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only }**
Parameter Description	**mac-address:** The MAC address of a static binding **Vlan-id:** The VLAN ID of a static binding. It indicates the outer VLAN ID of a QINQ-termination user. **ip-address:** The IP address of a static binding *interface-id***:** The Port ID (PID) of a static binding **wlan-id:** WLAN ID of a static binding **ip-mac:** IP-MAC based mode **ip-only:** IP-based mode
Configuration Mode	Global configuration mode
Usage Guide	Through this command, legitimate users can pass IP Source Guard detection instead of being controlled by DHCP. For a Fit AP in a wireless scenario, an AC cannot access static information of users that are connected to a wired port of a wireless AP.

Specifying an Exception VLAN for IP Source Guard

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	**vlan-id:** A VLAN ID exempted from IP Source Guard on a port
Command	Interface configuration mode/WLAN security configuration mode
Usage Guide	By using this command, the specified VLANs under a port where IP Source Guard function is enabled can be exempted from check and filtering.

Configuration Example

Enabling IP Source Guard on Port 1

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.

	Ruijie(config)# interface GigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# ip verify source Ruijie(config-if-GigabitEthernet 0/1)# end Ruijie(config)# wlansec 1 Ruijie(config-wlansec)# ip verify source port-security Ruijie(config-wlansec)# end
Verification	Displays the address filtering table of IP Source Guard.
	Ruijie# show ip verify source

Configuring a Static Binding

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard. ● Configure a static binding.
	Ruijie# configure terminal Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3 Ruijie(config)# end
Verification	Displays the address filtering table of IP Source Guard.
	Ruijie# show ip verify source NO. INTERFACE FilterType FilterStatus IPADDRESS MACADDRESS VLAN TYPE ----- ---------- ---------- ---------- ---------- ---------- ---- ---------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 Static 2 GigabitEthernet 0/1 IP-ONLY Active Deny-All 3 WLAN 1 IP-MAC Active Deny-All

Configuring a Static Binding of a QINQ-Termination Product

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard. ● Configure a static binding.

	Ruijie# configure terminal Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 inner-vlan 10 192.168.4.243 interface GigabitEthernet 0/3 Ruijie(config)# end
Verification	Displays the address filtering table of IP Source Guard.
	Ruijie# show ip verify source NO. INTERFACE FILTERTYPE FILTERSTATUS IPADDRESS MACADDRESS VLAN INNER-VLAN TYPE ----- ---------- ---------- ---------- ---------- ---------- -------- -------- ------- 1 GigabitEthernet 0/3 UNSET Inactive-restrict-off 192.168.4.243 00d0.f801.0101 1 10 Static

Specifying an Excluded VLAN

Configuration Steps	● Enable DHCP Snooping. ● Enable IP Source Guard.
	Ruijie(config)# interface GigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# ip verify source Ruijie(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1 Ruijie(config-if)# end Ruijie(config)# wlansec 1 Ruijie(config-wlansec)# ip verify source Ruijie(config-wlansec)# ip verify source exclude-vlan 1 Ruijie(config-wlansec)# end
Verification	Display the configuration of excluded VLANs specified on a port.
	Ruijie# show run

Common Errors

- Enable IP Source Guard on a trusted port under DHCP Snooping.
- Specify an excluded VLAN before IP Source Guard is enabled.

9.5 Monitoring

Displaying

Description	Command
Displays the address filtering table of IP Source Guard.	**show ip verify source** [**interface** *interface-id* | **wlan** *wlan-id*]
Displays the address binding database of IP Source Guard.	**show ip source binding**

10 Configuring DNS SNOOPING

10.1 Overview

DNS SNOOPING snoops the domain name server (DNS) packets exchanged between clients and servers to record the mapping table entries of domain names and IP addresses. It can also filter invalid DNS packets, including request packets from clients and response packets from servers.

DNS SNOOPING supports the following function:

Settings of authentication-free uniform resource locators (URLs), that is, domain name-based direct-through addresses.

Protocols and Standards

- RFC1034：DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

10.2 Applications

Application	Description
Applying Authentication-free URL	Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

10.2.1 Applying Authentication-free URL

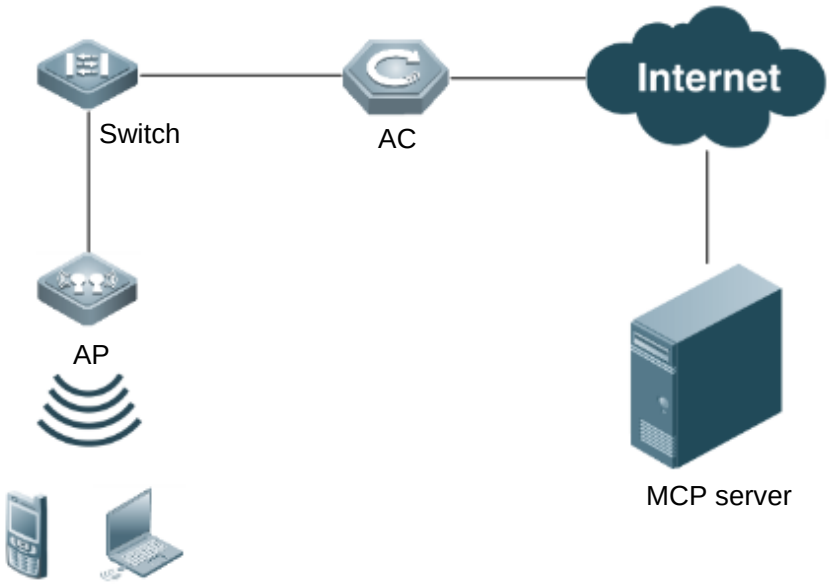
Scenario

As shown in Figure 10-1, the AC interacts with the MCP server, to implement the control on the network access right of unauthenticated downlink clients as well as their authentication via the authentication over WeChat following function.

Unauthenticated clients can access only WeChat, and can pass authentication by following the WeChat public account.

Authenticated clients have unrestricted network access rights.

Figure 10-1



Remarks:	Switch indicates a switch. AC indicates an access controller. AP indicates a wireless access point. MCP server is a cloud server.

Deployment

- Enable the authentication over WeChat following function on the AC for interaction with the MCP server.

10.3 Features

Basic Concepts

Authentication-free App

Unauthenticated clients can access authentication-free Apps, such as WeChat and Sina Weibo.

Authentication-free URL

Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

CWMP

CPE WAN Management Protocol (CWMP) is a technical standard initiated by Digital Subscriber's Line (DSL) forum and numbered TR-069. Therefore, CWMP is also known as TR-069 protocol. It provides the universal framework, message specification, method and data model for managing and configuring home network devices in next-generation networks.

The implementation of TR-069 protocol is complex. For App authentication, TR-069 provides the network channel for communication between the AC and the MCP server.

Overview

Feature	Description
Authentication-free URL	Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

10.3.1 Authentication-free URL

After the authentication-free URL function is enabled on the AC, unauthenticated clients are allowed to access specific URLs.

Working Principle

Unauthenticated clients cannot access the network normally when the Web-based authentication function is enabled on the AC. With the authentication-free URL function enabled, if the AC determines that traffic of an unauthenticated client contains the URL characteristics, the AC allows the traffic to pass and the client can access the specific URL without authentication.

10.4 Configuration

Configuration	Description and Command	
Configuring authentication-free URL.	⚠ (Mandatory) It is used to configure authentication-free Apps in global configuration mode.	
	free-url	Configures the authentication-free URL. At present, only WeChat, Sina App, certain iPhone Apps, and designated URLs are supported.
	ip dns snooping enable	Enables DNS SNOOPING.

10.4.1 Configuring Authentication-free URL

Configuration Effect

- Allow unauthenticated clients to access the configured authentication-free URL directly.

Notes

- The authentication-free URL takes effect only after the Web-based authentication function is enabled.

Configuration Steps

↘ Enabling DNS SNOOPING

- Mandatory.
- Enable DNS SNOOPING on the device.

Command	**ip dns snooping enable**
Parameter Description	N/A
Defaults	DNS SNOOPING is enabled by default.
Command Mode	Global configuration mode
Usage Guide	Run this command to enable DNS SNOOPING.

Configuring Authentication-free URL

- Mandatory.
- Configure an authentication-free URL on the AC.

Command	**free-url** { **weixin | sina | iphone | url** *url* }
Parameter Description	**weixin**: Indicates WeChat. **sina**: Indicates a Sina App. **iphone**: Indicates an iPhone App. *url*: Indicates a designated URL.
Defaults	No authentication-free URL is configured by default.
Command Mode	Global configuration mode
Usage Guide	You can configure multiple authentication-free URLs.

Verification

- Run the **show free-url** command to check the configuration status.
- Check whether unauthenticated clients can access the authentication-free URLs directly when the Web-based authentication function is enabled on the AC.

Configuration Example

Configuring WeChat as Authentication-free URL on AC

Configuration Steps	• Enter the global configuration mode. • Configure WeChat as an authentication-free URL.
Device	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#ip dns snooping enable Ruijie(config)# free-url weixin Ruijie(config)# free-url *.baidu.com Ruijie(config)#exit

Verification	Run the **show free-url** command to check the authentication-free URL information.
Device	

```
Ruijie(config)#show free-url
Total number of domain name   : 4
Total number of ip address    : 11


====================== free-url domain name table ========================
Host                    type
*.qpic.cn               weixin
*.weixin.qq.com         weixin
weixin.qq.com           weixin
*.baidu.com             url
==========================================================================


========================= free-url ip table ==============================
Host                    type    Address                         TTL(sec)
*.weixin.qq.com         weixin  61.151.224.41                    2118
                                140.207.135.125                 2118
                                140.207.54.47                   2118
*.qpic.cn               weixin  140.206.160.234                 2118
                                183.61.49.180                   151
                                101.226.129.204                 554
                                14.17.52.136                    16
weixin.qq.com           weixin  14.17.42.45                     800
*.baidu.com             url     115.239.210.246                 19
                                115.239.211.235                 2286
                                115.239.210.14                  284
==========================================================================
```

10.5 Monitoring

Clearing

Displaying

Description	Command
Displays authentication-free URLs.	**show free-url**
Clears authentication-free URLs.	**clear free-url**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs DNS SNOOPING.	**debug dns-snooping**

11 Configuring Port Security

11.1 Overview

Port security is used to restrict access to a port. Source MAC addresses of packets can be used to restrict the packets that enter the ports of a switch. You can set the number of static MAC addresses or the number of MAC addresses that are dynamically learned to restrict the packets that can enter the port. Ports enabled with port security are called secure ports.

11.2 Applications

Application	Description
Allowing Only Specified Hosts to Use Ports	For network security, certain ports of a device can be used only by specified hosts.

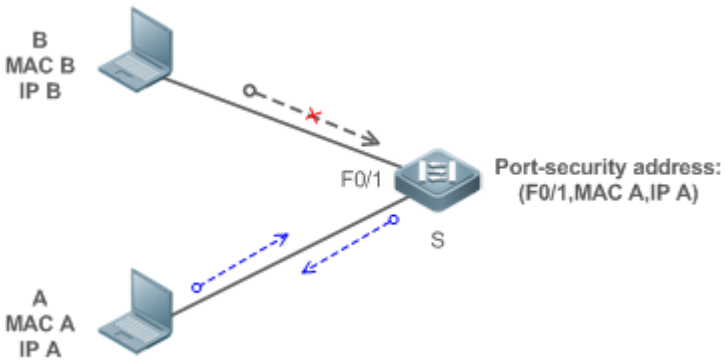
11.2.1 Allowing Only Specified Hosts to Use Ports

Scenario

In a scenario that has requirements for the network security, devices cannot be completely isolated physically. In this case, the devices need to be configured to restrict the PCs that connected to the ports of the devices.

- Only specified PCs can connect to the ports and normally use the network.
- Other PCs cannot use the network even if connected to the ports.
- After the configuration is complete, the administrator does not need to perform regular maintenance.

Figure 11-1



Remarks	S is the access device. A is a PC that can use the port F0/1. B is an unknown PC.

Deployment

- Enable ARP Check for port F0/1 (omitted).
- Enable port security on access device S and set the violation handling mode to protect.
- Set the maximum number of secure addresses allowed by port F0/1 to 1.
- Configure a static port security address on the port F0/1.

11.3 Features

Basic Concepts

Secure Port

Ports configured with port security are called secure ports. At present, Ruijie devices require that secure ports cannot be destination ports of mirroring.

Secure Addresses

Addresses bound to secure ports are called secure addresses. Secure addresses can be layer-2 addresses, namely MAC addresses, and can also be layer-3 addresses, namely, IP or IP+MAC addresses. When a secure address is bound to IP+MAC and a static secure MAC address is configured, the static secure MAC address must be the same as the MAC address bound to IP+MAC; otherwise, communication may fail due to inconsistency with the binding. Similarly, if only IP binding is set, only packets whose secure MAC addresses are statically configured or learned and whose source IP addresses are the bound IP address can enter the device.

Dynamic Binding

A method for a device to automatically learn addresses and convert learned addresses into secure addresses.

Static Binding

A command for manually binding secure addresses.

Aging of Secure Addresses

Regularly delete secure address records. Secure addresses for port security support aging configuration. You can specify only dynamically learned addresses for aging or specify both statically configured and dynamically learned secure addresses for aging.

Sticky MAC Address

Convert dynamically learned secure addresses into statically configured addresses. Addresses will not age. After the configurations are saved, dynamic secure addresses will not be learned again upon restart. If this function is not enabled, the secure MAC addresses dynamically learned must be learned again after device restart.

Security Violation Events

When the number of learned MAC addresses learned by a port exceeds the maximum number of secure addresses, security violation events will be triggered. You can configure the following modes for handing security violation events:

- protect: When security violation occurs, a corresponding secure port will stop learning MAC addresses and discard all packets of newly accessed users. This is the default mode for handling violation.
- restrict: When violation occurs, a port violation trap notification will be sent in addition to the behavior in the protect mode.
- shutdown: When violation occurs, the port will be disabled in addition to the behaviors in the preceding two modes.

Maximum Number of Secure Addresses

The maximum number of secure addresses indicates the total number of secure addresses statically configured and dynamically learned. When the number of secure addresses under a secure port does not reach the maximum number of secure addresses, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. If new users access the secure port in this case, security violation events will occur.

Overview

Feature	Description
Enabling Port Security	Creates a secure address list for a port.
Filtering Layer-2 Users	Processes the packets received by a port from non-secure addresses.
Filtering Layer-3 Users	Checks the layer-2 and layer-3 addresses of packets passing a port.
Aging of Secure Addresses	Regularly deletes secure addresses.

11.3.1 Enabling Port Security

Enable port security for a port to restrict packets that access the network through the port.

Working Principle

When port security is enabled, the device security module will check the sources of received packets. Only packets from addresses in the secure address list can be normally forwarded; otherwise, the packets will be discarded or the port performs other violation handling behaviors.

When the port security and 802.1x are configured at the same time, packets can enter a switch only when the MAC addresses of the packets meet the static MAC address configurations of 802.1x or port security. If a port is configured with a secure channel or is bound to global IP+MAC, packets in compliance with the secure channel or bound to global IP+MAC can avoid checking of port security.

Related Configuration

Enabling Port Security for a Port

By default, port security is disabled.

You can run the **switchport port-security** command to enable or disable the port security function for a port.

You cannot enable this function for a destination port of SPAN.

↘ Setting the Maximum Number of Secure Addresses for a Port

By default, the maximum number of secure addresses for a port is 128.

You can run the **switchport port-security maximum** command to adjust the maximum number of secure addresses for the port.

A smaller number of secure addresses mean fewer users that access the network through this port.

↘ Setting the Mode for Handling Violation

By default, when the number of secure addresses reaches the maximum number, the secure port will discard packets from unknown addresses (none of the secure addresses of the port).

You can run the **switchport port-security violation** command to modify the violation handling mode.

↘ Setting Secure Addresses That Can Be Dynamically Saved

By default, no secure address dynamically learned will be saved.

You can run the **switchport port-security mac-address sticky** command to save dynamically learned addresses to the configuration file. As long as the configuration file is saved, the device does not need to re-learn the secure addresses after the device is restarted.

11.3.2 Filtering Layer-2 Users

Set the secure addresses on a port to ensure that only devices whose MAC addresses are the same as the secure addresses can access the network through this port.

Working Principle

Add secure addresses for a secure port. When the number of secure addresses for a secure port does not reach the maximum number, the secure port can dynamically learn new dynamic secure addresses. When the number of secure addresses for the secure port reaches the maximum number, the secure port will not learn dynamic secure addresses any longer. The MAC addresses of users connecting to this port must be in the secure address list; otherwise, violation events will be triggered.

Related Configuration

↘ Adding Secure Addresses for a Secure port

By default, a port dynamically learns secure addresses. If an administrator has special requirements, the administrator can manually configure secure addresses.

You can run the **switch portport-security interface** command to add or delete secure addresses for a device.

11.3.3 Filtering Layer-3 Users

Add binding of secure addresses and check layer-2 and layer-3 addresses of packets passing a port.

Working Principle

Layer-3 secure addresses support only IP binding and IP+MAC binding, and supports only static binding (not dynamic binding).

When a layer-3 secure port receives packets, layer-2 and layer-3 addresses need to be parsed. Only packets whose addresses are bound are valid packets. Other packets are considered as invalid packets and will be discarded, but no violation event will be triggered.

Related Configuration

↘ Configuring Binding of Secure Addresses on Secure Ports

Binding of layer-3 secure addresses must be added manually.

You can run the **switchport port-security binding** command to add binding of secure addresses.

If only IP addresses are input, only IP addresses are bound. If IP addresses and MAC addresses are input, IP+MAC will be bound.

If only IP addresses are bound, the MAC addresses of packets are manually configured or dynamically learned. Only packets with bound IPs are allowed to enter the device.

If IP+MAC are bound, the MAC addresses of packets are manually configured or dynamically learned. Only packets with bound IP+MAC are allowed to enter the device.

11.3.4 Aging of Secure Addresses

Regularly delete secure addresses. When this function is enabled, you need to set the maximum number of secure addresses. In this way, the device can automatically add and delete secure addresses on this port.

Working Principle

Enable the aging timer to regularly query and delete secure addresses whose aging time expires.

Related Configuration

↘ Configuring Aging Time of Secure Addresses

By default, no secure address of a port will be aged.

You can run the **switchport port-security aging** command to enable aging time.

The **static** parameter can be used to age static addresses.

11.4 Configuration

Configuration	Description and Command	
Configuring Secure ports and Violation Handling Modes	(Mandatory) It is used to enable the port security service.	
	switchport port-security	Enables port security.
	switchport port-security maximum	Sets the maximum number of secure addresses for a port.
	switchport port-security violation	Configures the violation handling mode for port security.
	switchport port-security mac-address sticky	Configures automatic saving of dynamic addresses.
	switchport port-security preempt	Enables the secure address preemption function.
Configuring Secure Addresses on Secure Ports	(Optional) It is used to configure security filtering items.	
	switchport port-security mac-address	Configures the static secure addresses in the interface configuration mode.
	switchport port-security interface mac-address	Configures the static secure addresses in the global configuration mode.
	switchport port-security binding	Configures binding of secure addresses in the interface configuration mode.
	switchport port-security interface binding	Configures binding of secure addresses in the global configuration mode.
	switchport port-security aging	Configures aging time for all secure addresses on a port.

11.4.1 Configuring Secure ports and Violation Handling Modes

Configuration Effect

- Restrict the number of MAC addresses that can be learned from a port.
- Filter invalid packets based on MAC addresses, IP addresses or IP+MAC.

Notes

- A secure port cannot be the destination port of SPAN.
- The port security function cannot be configured for a DHCP Snooping trusted port.
- The port security function cannot be configured for excluded ports of global IP+MAC.
- The security function can be enabled only for wired switching ports and layer-2 AP ports in the interface configuration mode.

- The port security can work with other access control functions such as the 802.1x, global IP+MAC binding, and IP source guard. When these functions are used together, packets can enter a switch only when passing all security checks. If a security channel is configured for a port, packets in compliance with the security channel will avoid checking of the port security.

Configuration Steps

Enabling the Port Security Service

- Mandatory.
- If there is no special requirement, enable the port security service for a port on the access device.

Configuring the Maximum Number of Secure Addresses for a Port

- Optional. To adjust the maximum number of secure addresses running on a secure port, you can configure this item.
- Configure this item on a port enabled with port security.

Configuring Violation Handling Modes

- Optional. If you hope that other handling modes except discarding packets are implemented in case of violation, you can configure other handling modes.
- Configure this item on a port enabled with port security.

Saving Dynamically Learned Addresses

- Optional. If you hope that secure addresses are not re-learned after the device is restarted, you can configure this item.
- Configure this item on a port enabled with port security.

Enabling Secure Address Preemption

- Optional. If you hope that a static secure address can be successfully configured by forcing a dynamic secure address to get offline after the number of secure addresses reaches the maximum value, you can configure this feature.
- Configure this item on a port enabled with port security.

Verification

Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

Related Commands

Setting Port Security

Command	**switchport port-security**
Parameter Description	-
Command	Interface configuration mode

Mode	
Usage Guide	By using the port security feature, you can strictly control the input of a port of a device by restricting the MAC addresses and IP addresses (optional) that access the port.

Setting the Maximum Number of Secure Addresses for a Port

Command	**switchport port-security maximum** *value*
Parameter Description	*value*: Indicates the number of secure addresses, ranging from 1 to 128.
Command Mode	Interface configuration mode
Usage Guide	If you set the maximum number to 1 and configure a secure address for this port, the workstation (whose address is the configured secure address) connected to this port will exclusively use all bandwidth of the port.

Configuring the Violation Handling Mode for Port Security

Command	**switchport port-security violation** { **protect | restrict | shutdown** }
Parameter Description	**protect**: Discards violated packets. **restrict**: Discards violated packets and send trap notifications. **shutdown**: Discards packets and disables the port.
Command Mode	Interface configuration mode
Usage Guide	-

Saving Dynamic Secure Addresses to a Configuration File

Command	**switchport port-security mac-address sticky** *mac-address* [**vlan** *vlan-id*]
Parameter Description	*mac-address*: Indicates a static secure address. *vlan-id*: Indicates the VID of a MAC address.
Command Mode	Interface configuration mode
Usage Guide	-

Enabling Secure Address Preemption

Command	**switchport port-security preempt**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	After this function is enabled, a static secure address can be successfully configured by forcing a dynamic secure address (not fixed) to get offline after the number of secure addresses reaches the maximum value.

Configuration Example

Enabling Port Security for the Port gigabitethernet 0/3, Setting the Maximum Number of Addresses to 8, and Setting the Violation Handing Mode to protect

Configuration Steps	● Enable port security. ● Set the maximum number of secure addresses. ● Modify the violation handling mode.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security maximum 8 Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security violation protect Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security mac-address sticky Ruijie(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device.
	Ruijie# show port-security interface gigabitethernet 0/3 Interface : Gi0/3 Port Security: Enabled Port status : down Violation mode: Protect Maximum MAC Addresses:8 Total MAC Addresses:0 Configured MAC Addresses:0 Aging time : 0 mins SecureStatic address aging : Disabled

Common Errors

- Port security is enabled on a SPAN port.
- Port security is enabled on a DHCP trusted port.
- The configured maximum number of secure addresses is smaller than the number of existing secure addresses.

11.4.2 Configuring Secure Addresses on Secure Ports

Configuration Effect

- Allow specified users to use ports.
- Regularly update secure addresses of users.

Notes

- Sticky MAC addresses are special MAC addresses not affected by the aging mechanism. No matter dynamic or static aging is configured, sticky MAC addresses will not be aged.

Configuration Steps

Configuring Secure Addresses

- Optional. You need to manually add secure addresses for configuration.
- Configure this item on a port enabled with port security.

Configuring Binding of Secure Addresses

- Optional. You need to add layer-3 secure addresses for configuration.
- Configure this item on a port enabled with port security.

Configuring Aging Time

- Optional.
- Configure this item on a port enabled with port security.

Enabling Binding Filter Logging

- Optional.
- Enable binding filter logging in the global configuration mode.

Verification

- Run the command of the device for displaying the port security configurations to check whether the configurations take effect.

Related Commands

Adding Secure Addresses for Secure Ports in the Global Configuration Mode

Command	**switchport port-security interface** *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]
Parameter Description	*interface-id*: Indicates the interface ID. *mac-address*: Indicates a static secure address. *vlan-id*: Indicates the VID of a MAC address.
Command	Global configuration mode

Mode	
Usage Guide	-

Adding Secure Addresses for Secure Ports in the Interface Configuration Mode

Command	**switchportport-security mac-address** *mac-address* [**vlan** *vlan_id*]
Parameter Description	*mac-address*: Indicates a static secure address. *vlan-id*: Indicates the VID of a MAC address.
Command Mode	Interface configuration mode
Usage Guide	-

Adding Binding of Secure Addresses for Secure Ports in the Global Configuration Mode

Command	**switchport port-security interface** *interface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }
Parameter Description	*interface-id*: Indicates the interface ID. *mac-address*: Indicates a bound source MAC address. *vlan_id*: Indicates the VID of a bound source MAC address. *ipv4-address*: Indicates a bound IPv4 address. *ipv6-address*: Indicates a bound IPv6 address.
Command Mode	Global configuration mode
Usage Guide	-

Adding Binding of Secure Addresses for Secure Ports in the Interface Configuration Mode

Command	**switchport port-security binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }
Parameter Description	*mac-address*: Indicates a bound source MAC address. *vlan_id*: Indicates the VID of a bound source MAC address. *ipv4-address*: Indicates a bound IPv4 address. *ipv6-address*: Indicates a bound IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	-

Configuring Aging Time for All Secure Addresses on a Port

Command	**switchport port-security aging** { **static** | **time** *time* }
Parameter Description	**static**: Indicates that the aging time will be applied to manually configured secure addresses and automatically learned addresses; otherwise, the aging time will be applied to only automatically learned addresses. **time** *time*: Indicates the aging time of the secure addresses on this port, ranging from 0 to 1440 minutes. If it is set to 0, it indicates that the aging function is disabled actually.

Command Mode	Interface configuration mode
Usage Guide	-

Configuration Example

Configuring a Secure MAC Address 00d0.f800.073c for the Port gigabitethernet 0/3

Configuration Steps	● Enable port security. ● Add a secure address.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security mac-address 00d0.f800.073c vlan 1 Ruijie(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device.
	Ruijie# show port-security address NO. VLAN MacAddress PORT TYPE RemainingAge(mins) STATUS ---- ----- ---------- ---------- ---------- ---------- ---------- 1 1 00d0.f800.073c GigabitEthernet 0/3 Configured -- active

Configuring a Security Binding of the IP Address 192.168.12.202 for the Port gigabitethernet 0/3

Configuration Steps	● Enable port security. ● Add a binding of the secure address.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security binding 192.168.12.202 Ruijie(config-if-GigabitEthernet 0/3)# end

Verification	Check the port security configuration on the device.
	NO. VLAN MacAddress PORT IpAddress FilterType FilterStatus ---- ---- ---------- ---------- ---------- ---------- ---------- 1 -- -- Gi0/3 192.168.12.202 ipv4-only active

Configuring a Secure MAC Address 00d0.f800.073c and a Security Binding of the IP Address 0000::313b:2413:955a:38f4 for the Port gigabitethernet 0/3

Configuration Steps	• Enable port security. • Add a binding of the secure address.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitethernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport mode access Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security binding 00d0.f800.073c vlan 1 0000::313b:2413:955a:38f4 Ruijie(config-if)# end
Verification	Check the port security configuration on the device.
	ruijie#show port-security binding NO. VLAN MacAddress PORT IpAddress FilterType FilterStatus ---- ---- ---------- ---------- ---------- ---------- -------- 1 -- -- Gi0/3 192.168.12.202 ipv4-only active 2 1 00d0.f800.073c Gi0/3 ::313b:2413:955a:38f4 ipv6-mac active

Configuring the Aging Time of the Port gigabitethernet 0/3 to 8 Minutes, Which Is Also Applied to Statically Configured Secure Addresses

Configuration Steps	• Enable port security. • Configure aging time.
	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# interface gigabitthernet 0/3 Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security aging time 8 Ruijie(config-if-GigabitEthernet 0/3)# switchport port-security aging static

	Ruijie(config-if-GigabitEthernet 0/3)# end
Verification	Check the port security configuration on the device.
	Ruijie# show port-security gigabitethernet 0/3 Interface : Gi0/3 Port Security: Enabled Port status : down Violation mode:Shutdown Maximum MAC Addresses:8 Total MAC Addresses:0 Configured MAC Addresses:0 Aging time : 8 mins SecureStatic address aging : Enabled

11.5 Monitoring

Displaying

Description	Command
Displays all secure addresses or all secure addresses of a specified port.	**show port-security address** [**interface** *interface-id*]
Displays all bindings or all bindings of a specified port.	**show port-security binding** [**interface** *interface-id*]
Displays all valid secure addresses of ports and the security binding records of the ports.	**show port-security all**
Displays the port security configurations of an interface.	**show port-security interface** *interface-id*
Displays the statistics about port security.	**show port-security**

12 Configuring VRRP

12.1 Overview

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol.

VRRP adopts the master-backup design to ensure migration of functions from a Master router to a Backup one when the Master failed, without influencing internal and external data communication or modifying Local Area Network (LAN) configuration. A VRRP group maps multiple routers into a virtual router. VRRP ensures only one router at a moment on behalf of a virtual router transfers packets, which is the elected Master. If the Master fails, one of the Backup routers will replace it. Under VRRP, it seems that a host in a LAN uses only one router and the routing remains functional even when the first-hop router fails.

- VRRP is applicable to LAN scenarios which require the redundancy of routing egresses.

Protocols and Standards

- RFC2338: Virtual Router Redundancy Protocol
- RFC3768: Virtual Router Redundancy Protocol (VRRP)
- RFC5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

12.2 Applications

Application	Description
Routing Redundancy	Configure routers in a LAN as one VRRP group to achieve simple routing redundancy.
Load Balancing	Configure routers in a LAN as multiple VRRP groups to achieve traffic load balancing.

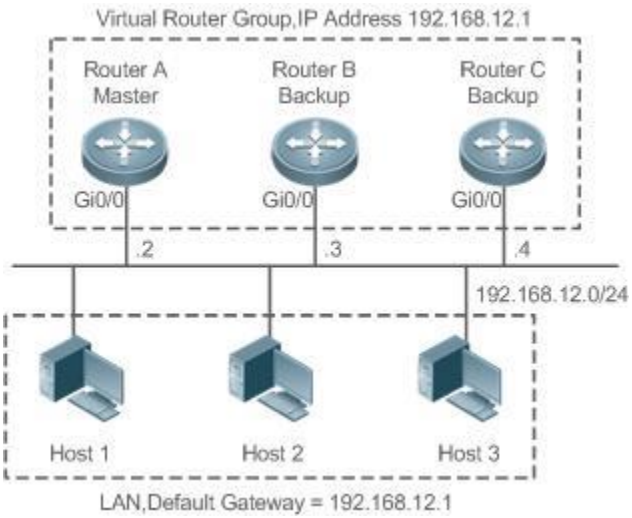
12.2.1 Routing Redundancy

Scenario

Configure routers in a LAN as one VRRP group, where hosts take the virtual IP address of this group as the default gateway address.

- Packets from Host 1, Host 2 and Host 3 to other networks are forwarded by the elected Master router (Router A in Figure 12-1).
- If Router A fails, the Master will be re-elected between Router B and Router C to forward packets, achieving simple routing redundancy.

Figure 12-1



Deployment

- Router A, Router B and Router C are connected to the LAN via Ethernet interfaces.
- On Router A, Router B and Router C, VRRP is configured on the Ethernet interfaces connected to the LAN.
- These Ethernet interfaces are in the same VRRP group whose virtual IP address is 192.168.12.1.
- The gateway address for Host 1, Host 2 and Host 3 is the IP address of the VRRP group, namely 192.168.12.1.

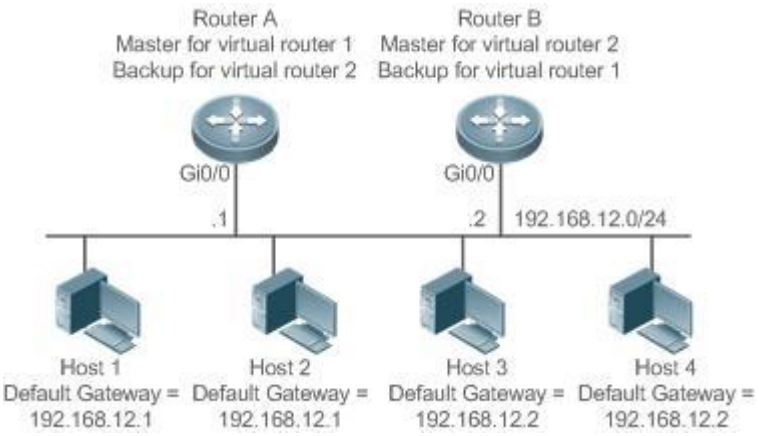
12.2.2 Load Balancing

Scenario

Configure routers in a LAN as multiple VRRP groups. Hosts in the LAN take virtual IP addresses of the groups as their gateways, and each router backs up for other routers in different group.

- Packets from Host 1 and Host 2 to other networks with the default gateway address as the virtual IP address of virtual router 1 are forwarded by the Master of virtual router 1 (Router A in Figure 12-2).
- Packets from Host 3 and Host 4 to other networks with the default gateway address as the virtual IP address of virtual router 2 are forwarded by the Master of virtual router 2 (Router B in Figure 12-2).
- Routing redundancy is achieved on Router A and Router B, and the LAN traffic is shared to achieve load balancing.

Figure 12-2



Deployment

- Router A and Router B are connected to the LAN via Ethernet interfaces.
- On Router A and Router B, two virtual routers are configured on the Ethernet interfaces connected to the LAN.

Router A takes the IP address 192.168.12.1 of Ethernet interface Gi0/0 as the IP address of virtual router 1. Thus for virtual router 1, Router A becomes the Master and Router B becomes the Backup.

- Router B takes the IP address 192.168.12.2 of Ethernet interface Gi0/0 as the IP address of virtual router 2. Thus for virtual router 2, Router B becomes the Master and Router A becomes the Backup.
- In the LAN, Host 1 and Host 2 take the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while Host 3 and Host 4 take the IP address 192.168.12.2 of virtual router 2 as the default gateway address.

12.3 Features

Basic Concepts

↘ Virtual Router

A virtual router, also called a VRRP group, is regarded as a default gateway for hosts in a LAN. A VRRP group contains a Virtual Router Identifier (VRID) and a set of virtual IP addresses.

↘ Virtual IP Address

Indicates the IP address of a virtual router. A virtual router can be configured with one or multiple IP addresses.

↘ IP Address Owner

If a VRRP group has the virtual IP address as that of an Ethernet interface on one real router, the router is regarded as the virtual IP address owner. In such case, the router priority is 255. If the owned Ethernet interface is available, the VRRP group will be in Master state automatically. The IP address owner receives and processes the packets with the destination IP address as that of the virtual router.

↘ Virtual MAC Address

The virtual MAC address of a VRRP group is an IEEE 802 MAC address, formatted as **00-00-5E-00-01-{VRID}** with the first five octets assigned and the last two as a group VRID. A VRRP group responds to an Address Resolution Protocol (ARP) request with its virtual MAC address instead of a real MAC address.

Master Router

In a VRRP group, only the Master router answers ARP requests and forwards IP packets. If a real router is the IP Address Owner, it becomes the Master router.

Backup Router

In a VRRP group, Backup routers only monitor the state of the Master but do not respond to ARP requests or forward IP packets. When the Master fails, Backup routers will take the chance to compete for the position.

Preemption Mode

If a VRRP group runs in Preemption mode, a higher priority Backup router will replace the lower priority Master router.

Overview

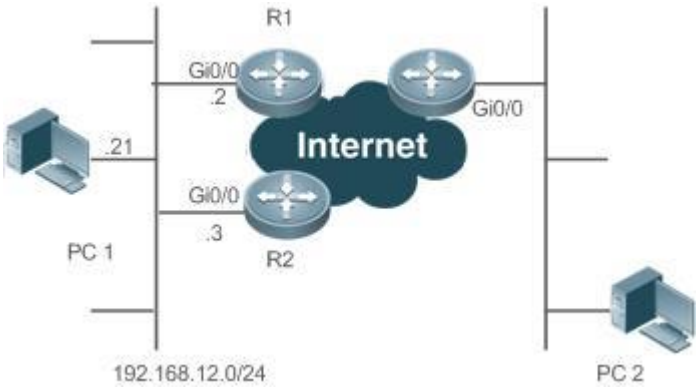
Feature	Description
VRRP	VRRP achieves redundancy for the default gateways of terminals on a multi-access media (for example, Ethernet). It enables a Backup router to forward packets when the Master router is down, providing transparent routing switch and promoting network service quality.

12.3.1 VRRP

In case that the Master router is faulty, VRRP achieves migration of functions from the Master router to a Backup one without influencing internal and external data communication or modifying LAN configuration.

Working Principle

Figure 12-3 Working Principle of VRRP



Working Mode of VRRP

The RFC2338, RFC3768 and RFC5798 protocols define the format and operating mechanism of VRRP packets. Multicast VRRP packets are sent periodically with specified destination addresses by the Master router to advertise normal operation or for Master election. VRRP allows a router in a LAN to automatically replace the Master who forwards IP packets when the latter fails. This helps achieve hot backup and fault tolerance of IP-based routing as well as ensure communication continuity and reliability for hosts in the LAN. A VRRP group achieves redundancy through multiple real routers. However, only one router acts as the Master to forward packets while the others are Backup routers. Router switching in a VRRP group is completely transparent to hosts in a LAN.

Master Election Process

The RFC standards stipulate the master election process as follows:

- VRRP provides a simple mechanism for Master election. First, compare the VRRP priorities configured on the interfaces of the routers in a VRRP group. The router with the highest priority is elected as the Master. If these priorities are equal, compare the primary IP addresses of these routers. The router with the biggest IP address is elected as the Master.
- After the Master router is elected, the other routers become Backup routers (and enter the **Backup** state) and monitor the state of the master router through the VRRP packets the master router sends. If the master router is operational, it regularly sends VRRP multicast packets known as Advertisement packets to notify the Backup routers of its status. If the Backup routers do not receive such packets within a set period, all of them will enter the Master state. In such case, the previous step of Master election is repeated. In this way, a router with the highest priority will be elected as a new master, achieving VRRP backup.

Once the Master router of a VRRP group is elected, it is responsible to forward packets for hosts in a LAN.

Communication Process

The VRRP communication process can be explained by Figure 12-3. The routers R1 and R2 are connected to the LAN segment 192.168.12.0/24 via the VRRP-enabled Ethernet interfaces Gi0/0. Hosts in the LAN take the virtual IP address of the VRRP group as the default gateway address. Only the virtual router is recognized by the hosts. The Master router in the group, however, is unknown. For example, when PC 1 plan to communicate with PC 2, PC 1 sends packets to the default gateway with the virtual IP address; The Master router in the group receives the packets and forwards them to PC 2. In this process, PC 1 only senses the virtual router instead of R1 or R2. The Master router in the group is elected between R1 and R2. When the Master fails, it will be replaced automatically by the other router.

Related Configuration

Enabling VRRP

By default, VRRP is disabled on an interface.

In the interface configuration mode, run the **vrrp** *group* **ip** *ipaddress* [**secondary**] or **vrrp** *group* **ipv6** *ipv6-address* command to set the VRID and virtual IP address to enable VRRP.

VRRP must be enabled on an interface.

Configuring the IPv4 VRRP Authentication String

By default, VRRP is in non-authentication mode.

Run the **vrrp group authentication** *string* command to set an authentication string in MD5 authentication mode or a plain text password in plain text mode for an IPv4 VRRP group. In the plain text authentication mode, a password contains 8 bytes at most.

Members of a VRRP group can communicate with each other only when they are in the same authentication mode. In the plain text authentication mode, all routers in a VRRP group should have the same authentication password. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations.

Configuring the VRRP Advertisement Interval

By default, the advertisement interval of the Master router is 1 second.

Run the **vrrp** [**ipv6**] *group* **timers advertise** *{ advertise-interval* | **csec** *centisecond-interval }* command to change the interval.

When VRRP learning timer is not configured, the same advertisement interval should be set for a VRRP group, otherwise routers in **Backup** state will discard received VRRP packets.

Configuring the VRRP Preemption Mode

By default, a VRRP group operates in the Preemption mode.

To enable the Preemption mode for a VRRP group, run the **vrrp** [**ipv6**] *group* **preempt** [**delay** *seconds*] command. The optional parameter **delay** *seconds* is 0 by default.

If a VRRP group operates in the Preemption mode, a router will become the Mater of the group when it finds that its priority is higher than that of the current Master. If a VRRP group operates in Non-preemption mode, a router will not become the Master even when it finds that its priority is higher than that of the current Master. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group. The optional parameter **Delay** *Seconds* defines the delay before a backup VRRP router declares its Master identity.

Enabling the IPv6 VRRP Accept Mode

By default, the Accept mode is disabled for an IPv6 VRRP group.

To enable the Accept mode, run the **vrrp ipv6** *group* **accept_mode** command.

After the Accept mode is enabled, an IPv6 VRRP virtual router in **Master** state receives and processes packets with the virtual router IP address as the destination; when the Accept mode is disabled, the virtual router discards such packets except Neighbor Advertisement (NA) packets and Neighbor Solicitation (NS) packets. Besides, an IPv6 VRRP master virtual router in **Owner** state receives and processes packets with the virtual router IP address as the destination by default no matter whether the Accept mode is configured or not.

Configuring the VRRP Router Priority

By default, the router priorities in a VRRP group are all 100.

To adjust the priority, run the **vrrp** [**ipv6**] *group* **priority** *level* command.

If a router in the Preemption mode owns the group's virtual IP address and the highest priority, it becomes the group Master, while the other routers with lower priorities in the group become Backup (or monitoring) routers.

Configuring the VRRP Tracked Interface

By default, no interface is tracked by a VRRP group.

To configure such an interface, run the **vrrp** *group* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-addess* } [*priority*] or **vrrp ipv6** ***group*** **track** *interface-type interface-number* **[** *priority* **]** command.

After an interface is configured for a VRRP group to monitor, the router priority will be adjusted dynamically based on the interface state. Once the interface becomes unavailable, the priority of the router in the group will be reduced by a set value, and another functional and higher priority router in this group will become the Master.

To trace the link layer protocol status of an interface, the **link** parameter needs to be configured. Otherwise, the network layer protocol status of the interface is traced.

Configuring the VRRP Tracked IP Address

By default, no IP address is tracked by a VRRP group.

To configure such an address, run the **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*] or **vrrp ipv6** *group* **track {** *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*] command.

After an IP address is configured for a VRRP group to monitor, the router priority will be adjusted dynamically based on the address accessibility. Once the address is inaccessible (the **ping** command fails), the priority of the router in the group will be reduced by a set value, and another higher priority router in this group will become the Master.

Configuring the VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group.

To enable it, run the **vrrp** [**ipv6**] *group* **timers learn** command.

After the learning timer is configured, a VRRP Backup router learns the advertisement interval of NA packets from the Master. Based on this instead of a locally set interval, the Backup router calculates the interval for determining a failure of the Master. This command achieves the synchronization of advertisement intervals between Backup routers and the Master.

Configuring the VRRP Group Description

By default, no description is configured for a VRRP group.

To configure such a string, run the **vrrp** [**ipv6**] *group* **description** *text* command.

A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the VRRP Delay

By default, no delay is configured for a VRRP group.

To enable it, run the **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* } command. The two types of delay range from 0 to 60 seconds.

The command configures the delay of starting a VRRP group on an interface. There are two types of VRRP delay: the delay after system startup and the delay after an interface resumes. You may configure them respectively or simultaneously. After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuring the IPv4 VRRP Version

By default, IPv4 adopts the VRRPv2 standard.

To specify the version for IPv4 VRRP, run the **vrrp** *group* **version** { **2 | 3** } command.

When the parameter value is set to 2, VRRPv2 is adopted; when the parameter value is set to 3, VRRPv3 is adopted.

Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

By default, IPv4 VRRP packets are sent to the first **Up** Sub VLAN interface of a Super VLAN.

To specify the first Sub VLAN in Up state of a Super VLAN to receive IPv4 VRRP packets, run the **vrrp detection-vlan first-subvlan** command; to specify a Sub VLAN, run the **vrrp detection-vlan** *subvlan-id* command. If VRRP and VRRP Plus are enabled simultaneously on a Super VLAN interface, VRRP packets are sent to all Up interfaces of the Sub VLANs under the Super VLAN.

Both the above configurations reduce VRRP packets and avoids influencing router performance and occupying network bandwidth. Yet the routers constituting an IPv4 VRRP group should be interconnected within the first UP Sub VLAN interface or a specified Sub VLAN of the Super VLAN.

12.4 Configuration

Configuration	Description and Command	
Configuring IPv4 VRRP	(Mandatory) It is used to enable IPv4 VRRP.	
	vrrp *group* **ip** *ipaddress* [**secondary**]	Enables IPv4 VRRP.
	(Optional) It is used to configure IPv4 VRRP parameters.	
	vrrp *group* **authentication** *string*	Configures the IPv4 VRRP authentication string.
	vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } [**multiplier** *interval*]	Configures the IPv4 VRRP advertisement interval and timeout times.
	vrrp *group* **preempt** [**delay** *seconds*]	Configures the IPv4 VRRP Preemption mode.

Configuration	Description and Command	
	vrrp *group* **priority** *level*	Configures the IPv4 VRRP router priority.
	vrrp *group* **track** *interface-type interface-number* [*priority*]	Configures the IPv4 VRRP tracked interface.
	vrrp *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv4 VRRP tracked IP address.
	vrrp *group* **timers learn**	Configures the IPv4 VRRP learning timer.
	vrrp *group* **description** *text*	Configures the IPv4 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv4 VRRP delay.
	vrrp *group* **version** { **2 | 3** }	Configures the IPv4 VRRP version.
	vrrp detection-vlan {first-subvlan | *subvlan-id***}**	Specifies a sub VLAN of a super VLAN to receive the IPv4 VRRP packets.
Configuring IPv6 VRRP	(Mandatory) It is used to enable IPv6 VRRP.	
	vrrp *group* **ipv6** *ipv6-address*	Enables IPv6 VRRP in interface configuration mode.
	(Optional) It is used to configure IPv6 VRRP parameters.	
	vrrp ipv6 *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	Configures the IPv6 advertisement interval and timeout times.
	vrrp ipv6 *group* **preempt** [**delay** *seconds*]	Configures the IPv6 VRRP Preemption mode.
	vrrp ipv6 *group* **accept_mode**	Enables the Accept mode for an IPv6 VRRP group.
	vrrp ipv6 *group* **priority** *level*	Configures the IPv6 VRRP router priority.
	vrrp ipv6 *group* **track** *interface-type interface-number* [**link**] [*interface–priority*]	Configures the IPv6 VRRP tracked interface.
	vrrp ipv6 *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv6 VRRP tracked IP address.
	vrrp ipv6 *group* **timers learn**	Configures the IPv6 VRRP learning timer.
	vrrp ipv6 *group* **description** *text*	Configures the IPv6 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv6 VRRP delay.

Configuration	Description and Command
Configuring VRRP-MSTP	The configuration is the same as IPv4 VRRP configuration.

12.4.1 Configuring IPv4 VRRP

Configuration Effect

- Configure a VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IP address.
- Configure multiple VRRP groups on an interface to achieve load balancing and offer more stable and reliable network services.
- Configure the VRRP tracked interfaces to monitor real-time failures, change interface priorities and realize master-backup failover dynamically.

Notes

- To achieve VRRP, the routers in a VRRP group should be configured with the same virtual IPv4 address.
- To achieve mutual backup between multiple IPv4 VRRP groups, configure multiple IPv4 VRRP groups with identical VRRP configuration on different interface and configure different priorities for them so that they act as the master and backup groups mutually.
- Enable VRRP on Layer-3 interfaces.

Configuration Steps

Enabling IPv4 VRRP

- By default, IPv4 VRRP is disabled on an interface. You can enable it based on your demand.

Configuring the IPv4 VRRP Authentication String

- By default, VRRP is in non-authentication mode. You can enable plain text authentication mode based on your demand.

Configuring the IPv4 VRRP Advertisement Interval

- By default, the Master router sends advertisement packets every one second. You can modify the interval based on your demand.

Configuring the IPv4 VRRP Preemption Mode

- By default, a VRRP group operates in Preemption mode with a zero-second delay.

Configuring the IPv4 VRRP Router Priority

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

Configuring the IPv4 VRRP Tracked Interface

- By default, an IPv4 VRRP group monitors no interface and the value of priority change is 10. To achieve fault monitoring through interface monitoring, please configure this item.

Configuring the IPv4 VRRP Learning Timer

- By default, the learning timer is disabled for a VRRP group. Enable this function if the Backup routers need to learn the Master's advertisement interval.

Configuring the IPv4 VRRP Group Description

- By default, no description is configured for a VRRP group. To distinguish VRRP groups clearly, configure descriptions.

Configuring the IPv4 VRRP Delay

- By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Configuring the IPv4 VRRP Version

- By default, IPv4 adopts the VRRPv2 standard. To change it, use the corresponding command.

Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

- By default, IPv4 VRRP packets are only sent to the first **UP** Sub VLAN interface of a Super VLAN, but you may configure a specific Sub VLAN.

Verification

- Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *ipaddress*: Indicates the IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode

Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations. This command is only applicable to VRRPv2 instead of VRRPv3. Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP) packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). ***csec*** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information. According to the RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode

Usage Guide	This command is used to manually configure the VRRP router priority.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. ***interval*** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. ***timeout*** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command	Interface configuration mode

Mode	
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and Backup routers.

Configuring the IPv4 VRRP Group Description

Command	**vrrp** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuring the IPv4 VRRP Version

Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

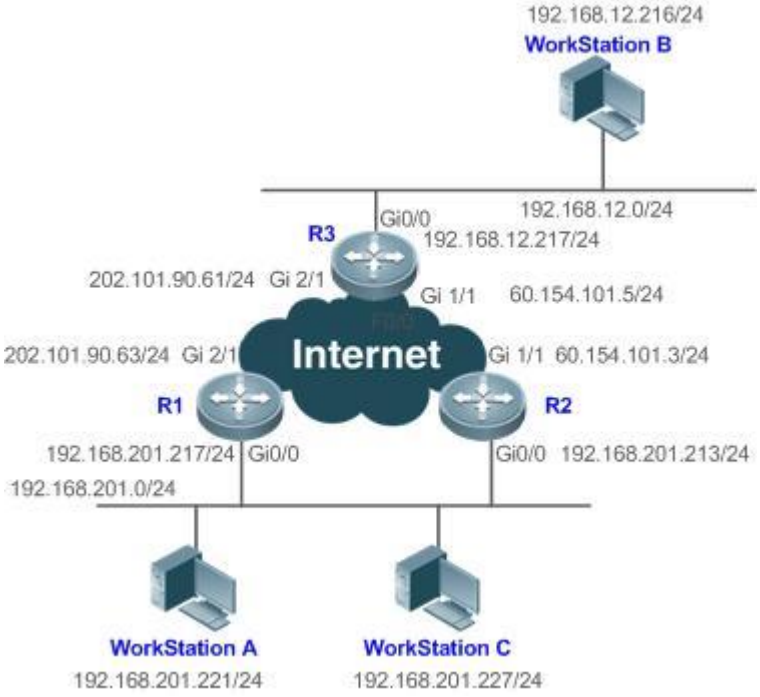
Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

Command	**vrrp detection-vlan first-subvlan**
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super VLAN.

Command Mode	Interface configuration mode
Usage Guide	This command is used to specify a Sub VLAN of a Super VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a Super VLAN using the following three methods. Packets are sent to the first UP Sub VLAN interface in a Super VLAN, or to a specified Sub VLAN interface in a Super VLAN, or to all the Sub VLAN interfaces in a Super VLAN. If VRRP and VRRP Plus are enabled simultaneously on a Super VLAN interface, VRRP packets are sent to all Up interfaces of the Sub VLANs under the Super VLAN. This command is configured on a VLAN interface and effective only to Super VLAN interfaces.

Configuration Example

Configuring an IPv4 VRRP Group and Tracked Interface

Scenario **Figure 12-4**	
Configuration Steps	● The cluster of Work Station A and Work Station B (192.168.201.0/24) uses the virtual IP address 192.168.201.1 of the VRRP group constituted by the routers R1 and R2 as the gateway address to communicate with Work Station B (192.168.12.0 /24). ● GigabitEthernet 2/1 on R1 is configured as the tracked interface. ● No VRRP but an ordinary routing function is configured on R3.
R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 0/0)#no switchport R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0

	R3(config-if-GigabitEthernet 0/0)#exit R3(config)#interface GigabitEthernet 1/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 1/1)#no switchport R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0 R3(config-if-GigabitEthernet 1/1)#exit R3(config)#interface GigabitEthernet 2/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 2/1)#no switchport R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit R3(config)#router ospf R3(config-router)#network 202.101.90.0 0.0.0.255 area 10 R3(config-router)#network 192.168.12.0 0.0.0.255 area 10 R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0 R1(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120 R1(config-if-GigabitEthernet 0/0)#vrrp 1 version 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 2/1 30 R1(config-if-GigabitEthernet 0/0)#exit R1(config)#interface GigabitEthernet 2/1 R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 2/1)#exit R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal

```
R2(config)#interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)#vrrp 1 version 3
R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)#exit
R2(config)#interface GigabitEthernet 1/1
// The command “no switchport” is only required for a switch.
R2(config-if-GigabitEthernet 1/1)#no switchport
R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)#exit
R2(config)#router ospf
R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
```

Verification

Run the **show vrrp** command to verify the configuration.

- Check whether R1, which acts as the Master, reduces its VRRP priority from 120 to 90 when GigabitEthernet2/1 connected to the Wide Area Network (WAN) is unavailable. If yes, R2 becomes the Master.
- Check whether R1 resumes its VRRP priority from 30 to 120 when GigabitEthernet 2/1 connected to the WAN recovers. If yes, R1 is re-elected as the Master.

R1

```
R1#show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
    Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
   Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
```

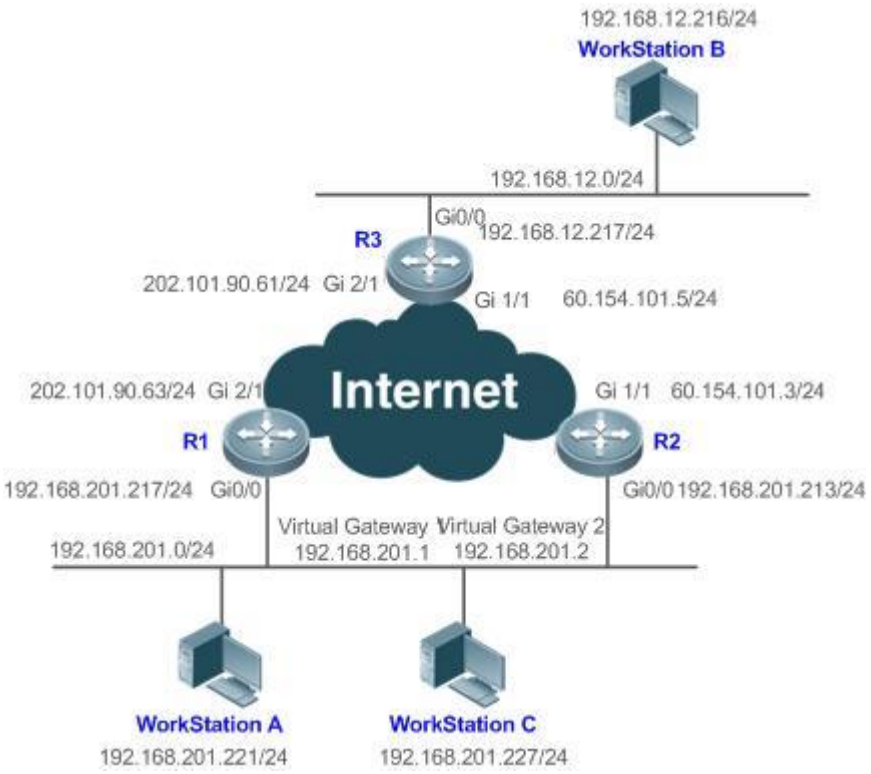
	up GigabitEthernet 2/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/0 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.
- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

Configuration Example

Configuring Multiple IPv4 VRRP Groups

Scenario **Figure 12-5**	
Configuration Steps	● The user workstation cluster (192.168.201.0/24) uses the backup group constituted by the routers R1 and R2. The gateway for partial workstations (A for example) points to the virtual IP address 192.168.201.1 of the backup group 1, while that for other partial workstations (C for example) points to the virtual IP address 192.168.201.2 of the backup group 2. IPv4 multicast routing is enabled on all the routers. ● R1 acts as the master router in the group 2 and as a backup router in the group 1. ● R2 acts as a backup router in the group 2 and as a master router in the group 1.
R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 0/0)#no switchport R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0 R3(config-if-GigabitEthernet 0/0)#exit R3(config)#interface GigabitEthernet 1/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 1/1)#no switchport R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0

	R3(config-if-GigabitEthernet 1/1)#exit R3(config)#interface GigabitEthernet 2/1 // The command “no switchport” is only required for a switch. R3(config-if-GigabitEthernet 2/1)#no switchport R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit R3(config)#router ospf R3(config-router)#network 202.101.90.0 0.0.0.255 area 10 R3(config-router)#network 192.168.12.0 0.0.0.255 area 10 R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0 R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/0)#vrrp 2 priority 120 R1(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3 R1(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2 R1(config-if-GigabitEthernet 0/0)#vrrp 2 track GigabitEthernet 2/1 30 R1(config-if-GigabitEthernet 0/0)#exit R1(config)#interface GigabitEthernet 2/1 R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 2/1)#exit R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0 R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1 R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3

	R2(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120 R2(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2 R2(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3 R2(config-if-GigabitEthernet 0/0)#exit R2(config)#interface GigabitEthernet 1/1 R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 1/1)#exit R2(config)#router ospf R2(config-router)#network 60.154.101.0 0.0.0.255 area 10 R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether R1, which acts as a master router in the group 2, reduces its VRRP group priority from 30 to 90 when it finds that the interface GigabitEthernet 2/1 connected to a WAN is unavailable. If yes, R2 in the group 2 becomes a master router. ● Check whether R1 increases its VRRP group priority from 30 to 120 when it finds the interface GigabitEthernet 2/1 connected to a WAN becomes available again. If yes, R1 becomes a master router again in the group 2.
R1	R1#show vrrp GigabitEthernet 0/0 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec GigabitEthernet 0/0 - Group 2 State is Master Virtual IP address is 192.168.201.2 configured

	Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up: up GigabitEthernet 2/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/0 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.213 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec GigabitEthernet 0/0 - Group 2 State is Backup Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120

	Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.
- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

12.4.2 Configuring IPv6 VRRP

Configuration Effect

- Configure an IPv6 VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IPv6 address.
- Configure multiple IPv6 VRRP groups on an interface to achieve load balance and achieve more stable and reliable network services.
- Configure the VRRP tracked interfaces to monitor real-time failures, change interface priorities and realize master-backup failover dynamically.

Notes

- To achieve VRRP, the routers in a VRRP group should be configured with the same virtual IPv6 address.
- To achieve mutual backup for multiple IPv6 VRRP backup groups, you need to configure multiple IPv6 VRRP groups with identical VRRP configuration on an interface and configure different priorities for them to make routers master and backup mutually.
- VRRP must be enabled on Layer-3 interfaces.
- To use the IPv6 VRRP function on a N18000 device with a CB line card inserted, enable the IPv6 VRRP function in global configuration mode first.

Configuration Steps

↘ Enabling IPv6 VRRP in Interface Configuration Mode

- By default, IPv6 VRRP is not enabled on an interface. You can enable it based on your demand.

↘ Configuring the IPv6 VRRP Advertisement Interval

- By default, the Master router sends advertisement packets every one second. You can modify the interval based on your demand.

Configuring the IPv6 VRRP Preemption Mode

- By default, a VRRP group operates in Preemption mode with a zero-second delay.

Enabling the Accept Mode for an IPv6 VRRP Group

- By default, the Accept mode is disabled for an IPv6 VRRP group. To require an IPv6 VRRP VRRP group in Master state to receive and process packets with the destination IP address as that of the virtual router, enable Accept mode.

Configuring the IPv6 VRRP Router Priority

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

Configuring the IPv6 VRRP Tracked Interface

- By default, no tracked interface is configured. You can modify the interval based on your demand.

Configuring the IPv6 VRRP Tracked IP Address

- By default, no tracked IPv6 address is configured and the value of priority change is 10. You can configure this function based on your demand.

Configures the IPv6 VRRP Learning Timer

- By default, the learning timer is disabled for a VRRP group. Enable this function if the Backup routers need to learn the Master's advertisement interval.

Configuring the IPv6 VRRP Group Description

- By default, no description is configured for a VRRP group. To distinguish VRRP groups clearly, configure descriptions.

Configuring the IPv4 VRRP Delay

- By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Verification

- Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv6 VRRP

Command	**vrrp** *group* **ipv6** *ipv6-address*
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *ipv6-address*: Indicates the IPv6 address of a VRRP group.
Command	Interface configuration mode

Mode	
Usage Guide	IPv6 VRRP groups and IPv4 VRRP groups share a VRID range from 1 to 255. One VRID is applicable to an IPv4 VRRP group and an IPv6 VRRP group at the same time. The first configured address should be a link-local address, which can be deleted only after other virtual addresses.

Configuring the IPv6 VRRP Advertisement Interval

Command	**vrrp ipv6** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). ***csec*** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information. According to the RFC standards, if an IPv6 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.

Configuring the Preemption Mode

Command	**vrrp ipv6** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

Enabling the Accept Mode for an IPv6 VRRP Group

Command	**vrrp ipv6** *group* **accept_mode**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	By default, an IPv6 VRRP group in **Master** state is not permitted to receive packets with the destination IPv6 address as that of the VRRP group. However, it receives NA and NS packets no matter whether Accept

	mode is configured. Besides, the IP Address Owner in Master state receives and processes the packets with the destination IPv6 address as that of the VRRP group no matter whether Accept mode is configured or not.

Configuring the IPv6 VRRP Router Priority

Command	**vrrp ipv6** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of a VRRP router.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

Configuring the IPv6 VRRP Tracked Interface

Command	**vrrp ipv6** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv6 VRRP Tracked IP Address

Command	**vrrp ipv6** *group* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv6-global-addres*: Indicates the IPv6 global unicast address. *ipv6-linklocal-address*: Indicates the IPv6 link-local address. *interface-type interface-number*: Indicates the interface to be tracked. ***interval*** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. ***timeout*** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for *retry-value* times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The

	default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv6 address for an IPv6 VRRP group. If the host IP address being tracked is a link-local address, specify a network interface. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configures the IPv6 VRRP Learning Timer

Command	**vrrp ipv6** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and Backup routers.

Configuring the IPv6 VRRP Group Description

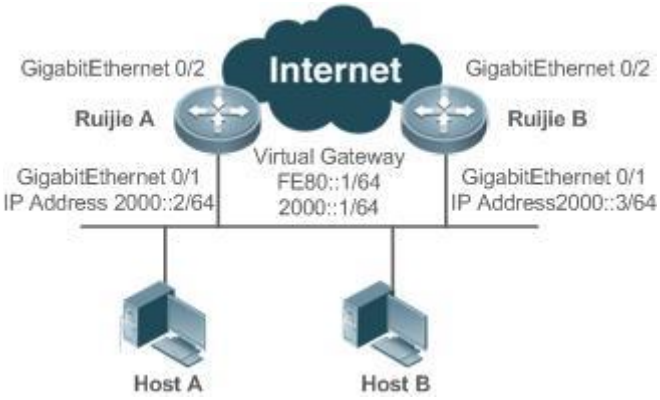
Command	**vrrp ipv6** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuration Example

Configuring an IPv6 VRRP Group and Tracked Interface

Scenario **Figure 12-6**	
Configuration Steps	● Host A and Host B access the Internet resources through the default gateway 2000::1/64. ● Ruijie A and Ruijie B belong to the IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively. ● Ruijie A tracks the interface GigabitEthernet 0/2 connected to the Internet. When GigabitEthernet 0/2 is unavailable, Ruijie A reduces its priority and Ruijie B acts as a gateway.
RuijieA	RuijieA#configure terminal RuijieA(config)#interface GigabitEthernet 0/1 RuijieA(config-if-GigabitEthernet 0/1)#no switchport RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64 RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 track GigabitEthernet 0/2 50 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
RuijieB	RuijieB#configure terminal RuijieB(config)#interface GigabitEthernet 0/1 RuijieB(config-if-GigabitEthernet 0/1)#no switchport RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64 RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3

	RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether Ruijie A, which acts as the Master router, reduces its VRRP group priority from 120 to 70 when it finds that the interface GigabitEthernet 0/2 connected to WAN is unavailable. If yes, Ruijie B becomes the Master. ● Check whether Ruijie A increases its VRRP group priority from 50 to 120 when it finds the interface GigabitEthernet 0/2 connected to WAN becomes available again. If yes, Ruijie A becomes the Master again.
RuijieA	RuijieA#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1 State is Master Virtual IPv6 address is as follows: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 120 Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up: up GigabitEthernet 0/2 priority decrement=50
RuijieB	RuijieB#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1 State is Backup Virtual IPv6 address is as follow: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201

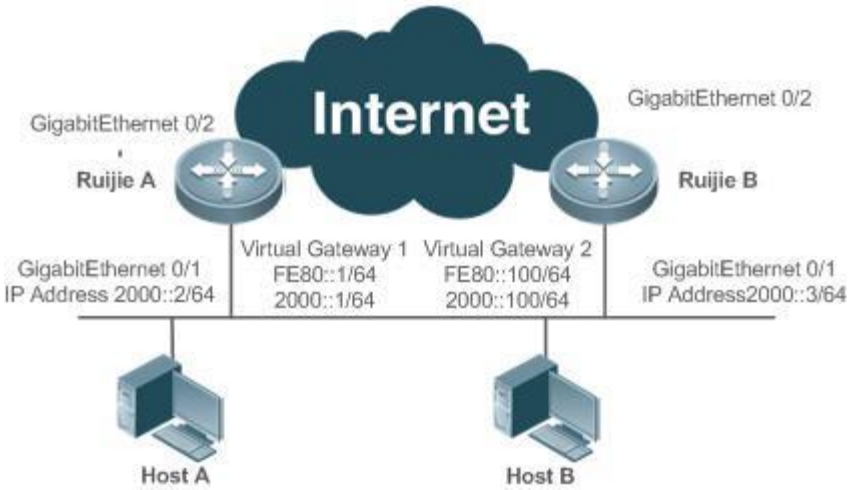
	Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 100 Master Router is FE80::1234, priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

Configuration Example

↘ Multiple VRRP Backup Groups (under IPv6)

Scenario **Figure 12-7**	
Configuration Steps	● Host A and Host B access the Internet resources through the gateways 2000::1/64 and 2000::100/64 respectively. ● Ruijie A and Ruijie B belong to the IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively. ● Ruijie A and Ruijie B belong to the backup group 2 of a virtual IPv6 router, and their virtual addresses are 2000::100/64 and FE80::100 respectively. ● Ruijie A and Ruijie B act as gateways and forward flows, being a backup router to each other.

RuijieA	RuijieA#configure terminal RuijieA(config)#interface GigabitEthernet 0/1 RuijieA(config-if-GigabitEthernet 0/1)#no switchport RuijieA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64 RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 RuijieA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode RuijieA(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 RuijieA(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 100 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 RuijieA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
RuijieB	RuijieB#configure terminal RuijieB(config)#interface GigabitEthernet 0/1 RuijieB(config-if-GigabitEthernet 0/1)#no switchport RuijieB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64 RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 RuijieB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode RuijieB(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 RuijieB(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 120 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 RuijieB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
Verification	Run the **show vrrp** command to verify the configuration.
RuijieA	RuijieA#show ipv6 vrrp

	GigabitEthernet 0/1 - Group 1 State is Master Virtual IPv6 address is as follows: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 120 Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec GigabitEthernet 0/1 - Group 2 State is Backup Virtual IPv6 address is as follows: FE80::100 2000::100 Virtual MAC address is 0000.5e00.0202 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 100 Master Router is FE80::5678, priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec
RuijieB	RuijieB#show ipv6 vrrp GigabitEthernet 0/1 - Group 1 State is Backup

```
  Virtual IPv6 address is as follow:
    FE80::1
    2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
GigabitEthernet 0/1 - Group 2
  State is Master
  Virtual IPv6 address is as follows:
    FE80::100
    2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::5678(local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

12.4.3 Configuring VRRP-MSTP

Configuration Effect

- Link-level and gateway-level backup are achieved and network robustness is improved greatly when MTSP and VRRP are applied simultaneously.

Notes

- configure the routers in a VRRP backup group with the same virtual IPv4 address.
- Enabled VRRP on a Layer 3 interface.

Configuration Steps

Enabling IPv4 VRRP

- By default, IPv4 VRRP is not enabled on an interface. To enable IPv4 VRRP, please configure this item.

Configuring the IPv4 VRRP Authentication String

- By default, VRRP is in a non-authentication mode. To enable plain text password authentication for VRRP, please configure this item.

Configuring the IPv4 VRRP Advertisement Interval

- By default, a master router sends VRRP GWADV packets at an interface of one second. To manually set a value, please configure this item.

Configuring the IPv4 VRRP Preemption Mode

- By default, VRRP groups work in the preemption mode with zero-second delay.

Configuring the IPv4 VRRP Router Priority

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

Configuring the IPv4 VRRP Tracked Interface

- By default, an IPv4 VRRP group monitors no interface. To achieve fault monitoring through monitoring an interface, please configure this item.

Configuring the IPv4 VRRP Learning Timer

- By default, timed learning is not enabled for a VRRP backup group. To enable backup routers to learn the VRRP GWADV packets from a master router, please configure this item.

Configuring the IPv4 VRRP Group Description

- By default, no description is configured for a VRRP group. To distinguish VRRP groups conveniently, please configure this item.

Configuring the IPv4 VRRP Delay

- By default, the VRRP delay for a VRRP group is not configured. Configure the delay to guarantee a stable transition from Non-preemption mode to Preemption mode.

Configuring the IPv4 VRRP Version

- By default, the VRRPv2 standard is adopted for IPv4 VRRP packets. To modify it manually, please configure this item.

Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

- By default, IPv4 VRRP packets are only sent to the first UP Sub VLAN interface in a Super VLAN, but you may configure a specific Sub VLAN interface to send such packets.

Verification

- Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *Ipaddress*: The IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations. This command is only applicable to VRRPv2 instead of VRRPv3. Authentication is abolished for VRRPv3 packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). ***csec*** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information. According to the RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the priority of a VRRP group.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command	Interface configuration mode

Mode	
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. ***interval*** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. ***timeout*** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and Backup routers.

Configuring the IPv4 VRRP Group Description

Command	**vrrp** *group* **description** *text*
Parameter	*group*: Indicates the VRID of a VRRP group.

Description	*text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuring the IPv4 VRRP Version

Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

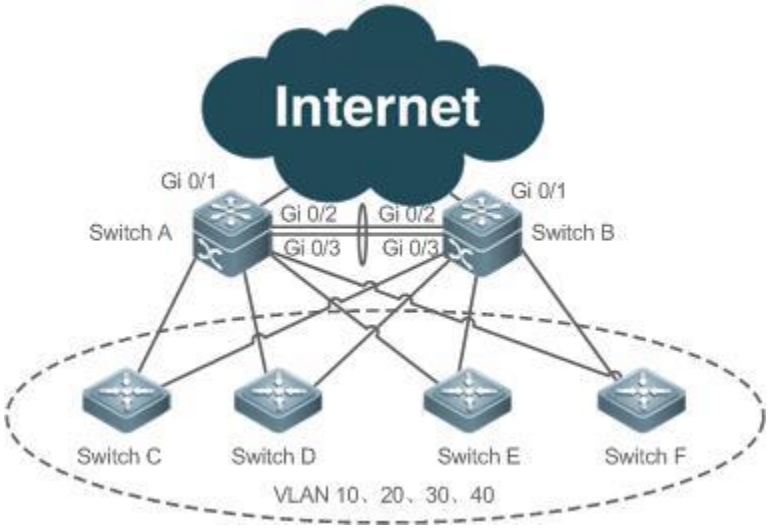
Command	**vrrp detection-vlan first-subvlan**
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super VLAN.
Command Mode	Interface configuration mode
Usage Guide	This command is used to specify a Sub VLAN of a Super VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a Super VLAN using the following two methods. Packets are sent to the first UP Sub VLAN interface in a Super VLAN, or to all the Sub VLAN interfaces in a Super VLAN. If both VRRP and VRRP PLUS are enabled on a Super VLAN interface, VRRP packets are sent to the first UP Sub VLAN interface in a Super VLAN. This command is configured on a VLAN interface and effective only to Super VLAN interfaces.

Configuration Example

Configuring VRRP+MSTP

Scenario

Figure 12-8



Configuration Steps

- Enable MSTP on routers (switches A, B, C, D, E and F in this example). Configure VLAN-Instance mapping (mapping VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0), and configure gateways (Switch A and Switch B in this example) as the root bridges of corresponding instances.
- Add the SVIs of all VLANs to corresponding VRRP backup groups, and configure gateways as the master and backup routers for corresponding backup groups See configuration details in the following table.

Gateway	VLAN ID	SVI	Backup Group	Virtual IP Address	State
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- Configure the uplink port (port Gi 0/1 of Switch A and Switch B) of master routers as a monitored interface of master router.
- Step 1: Create VLAN. Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 respectively on Switch A and Switch B.
- Step 2: Configure MST regions. Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to

	Instance 2, and the rest VLANs to Instance 0. ● Step 3: Configure Switch A as the root bridge for MST 0 and MST 1, and Switch B as the root bridge for MST 2. ● Step 4: Enable MSTP. ● Step 5: Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups. See configuration in the above table. ● Step 6: Configure master routers and backup routers for all the groups. ● Step 7: Configure the uplink ports of master routers as monitored ports of VRRP groups. Caution: Monitored ports should be Layer 3 ports. Step 8: Configure the Internet interfaces of the core routers as AP interfaces.
SwitchA	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch A. SwitchA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#vlan range 10,20,30,40 SwitchA(config-vlan-range)#exit //Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0. SwitchA(config)#spanning-tree mst configuration SwitchA(config-mst)#instance 1 vlan 10,20 %Warning:you must create vlans before configuring instance-vlan relationship SwitchA(config-mst)#instance 2 vlan 30,40 %Warning:you must create vlans before configuring instance-vlan relationship SwitchA(config-mst)#exit //On Switch A, configure the priority of MST 0 and MST 1 as 4096, and that of MST 2 as 8192. SwitchA(config)#spanning-tree mst 0 priority 4096 SwitchA(config)#spanning-tree mst 1 priority 4096 SwitchA(config)#spanning-tree mst 2 priority 8192 //Enabling MSTP SwitchA(config)#spanning-tree Enable spanning-tree. //Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups. SwitchA(config)#interface vlan 10

```
SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)#exit
SwitchA(config)#interface vlan 40
SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)#exit
//Increase the priority of the VRRP 10 and VRRP 20 of Switch A to 120.
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
SwitchA(config-if-VLAN 20)#exit
//Configure the Gi 0/1 port of Switch A as Route Port and its IP address as10.10.1.1/24.
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
//Configure the Gi 0/1 port of Switch A as a monitored port for VRRP 10 and VRRP 20, and a Priority decrement of 30.
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)#exit
```

	SwitchA(config)#interface vlan 20 SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30 SwitchA(config-if-VLAN 20)#exit //Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports. SwitchA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#interface range gigabitEthernet 0/2-3 SwitchA(config-if-range)#port-group 1 SwitchA(config)#interface aggregateport 1 SwitchA(config-if-AggregatePort 1)#switchport mode trunk
SwitchB	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch B. SwitchB#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)#vlan range 10,20,30,40 SwitchB(config-vlan-range)#exit //Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0. SwitchB(config)#spanning-tree mst configuration SwitchB(config-mst)#instance 1 vlan 10,20 %Warning:you must create vlans before configuring instance-vlan relationship SwitchB(config-mst)#instance 2 vlan 30,40 %Warning:you must create vlans before configuring instance-vlan relationship SwitchB(config-mst)#exit //On Switch B, configure the priority of MST 2 as 4096, and that of MST 0 and MST 1 as 8192. SwitchB(config)#spanning-tree mst 2 priority 4096 SwitchB(config)#spanning-tree mst 0 priority 8192 SwitchB(config)#spanning-tree mst 1 priority 8192 //Enabling MSTP SwitchB(config)#spanning-tree Enable spanning-tree. //Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.

```
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
//Increase the priority of VRRP 30 and VRRP 40 of Switch B to 120.
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
SwitchB(config-if-VLAN 40)#exit
//Configure the Gi 0/1 port of Switch B as Route Port and its IP address as 10.10.1.1/24.
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#no switchport
SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)#exit
//Configure the Gi 0/1 port of Switch B as a monitored port for VRRP 30 and VRRP 40, and the Interface-Priority as 30.
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30
```

	SwitchB(config-if-VLAN 30)#exit SwitchB(config)#interface vlan 40 SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30 SwitchB(config-if-VLAN 40)#exit //Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports. SwitchB #configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchB (config)#interface range gigabitEthernet 0/2-3 SwitchB (config-if-range)#port-group 1 SwitchB (config)#interface aggregateport 1 SwitchB (config-if-AggregatePort 1)#switchport mode trunk
Verification	
Switch A	Check the configuration. SwitchA#show running-config ! vlan 10 ! vlan 20 ! vlan 30 ! vlan 40 ! spanning-tree spanning-tree mst configuration instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094 instance 1 vlan 10, 20 instance 2 vlan 30, 40 spanning-tree mst 0 priority 4096 spanning-tree mst 1 priority 4096 spanning-tree mst 2 priority 8192 interface GigabitEthernet 0/1

```
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
```

```
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
//Check VRRP status.
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
//Disconnect the uplink of Switch A, and check VRRP status.
SwitchA#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   90   3      -    P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   90   3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

Switch B

```
//Check the configuration.
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
```

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
```

```
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
//Check VRRP status.
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
//Disconnect the uplink of Switch B, and check VRRP status.
SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.
- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

12.5 Monitoring

Displaying

Description	Command
Displays the brief or detailed information of IPv4/IPv6 VRRP.	**show** [**ipv6**] **vrrp** [**brief** | *group*]
Displays the information of an IPv4/IPv6 VRRP group on a specified interface.	**show** [**ipv6**] **vrrp interface** *type number* [**brief**]
Displays the statistics of VRRP packets.	**show vrrp packet statistics** [*interface-type interface-number*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs VRRP errors, events, packets and status.	**debug** [**ipv6**] **vrrp**
Debugs VRRP errors.	**debug** [**ipv6**] **vrrp errors**
Debugs VRRP events.	**debug** [**ipv6**] **vrrp events**
Debugs VRRP packets.	**debug vrrp packets** [**acl** *acl-id* **|** [**icmp | protocol**] **interface** *type number* [*group*]] **debug ipv6 vrrp packets** [**acl** *acl-name* **|** [**icmp | protocol**] **interface** *type number* [*group*]]
Debugs VRRP status.	**debug** [**ipv6**] **vrrp state**

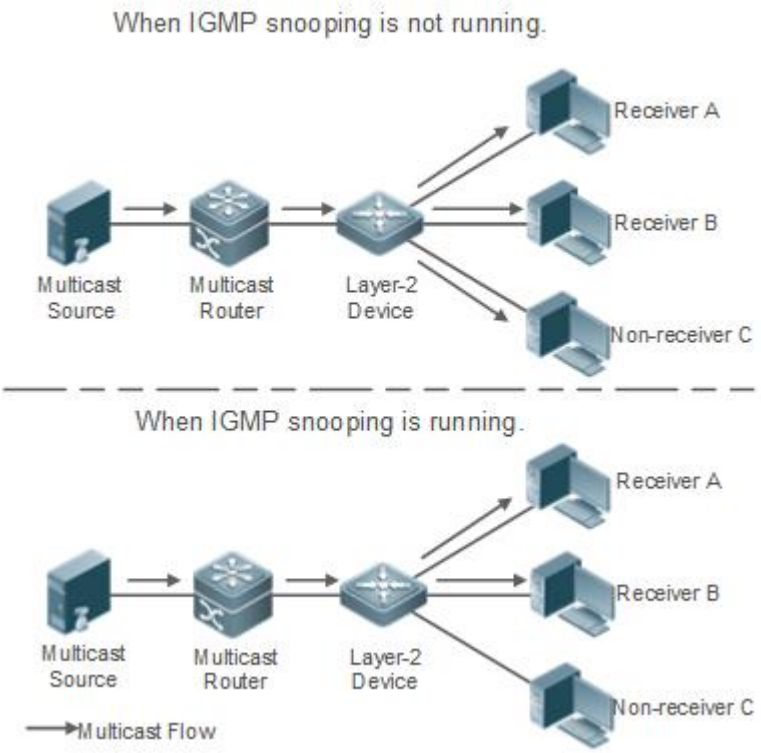
13 Configuring IGMP Snooping

13.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

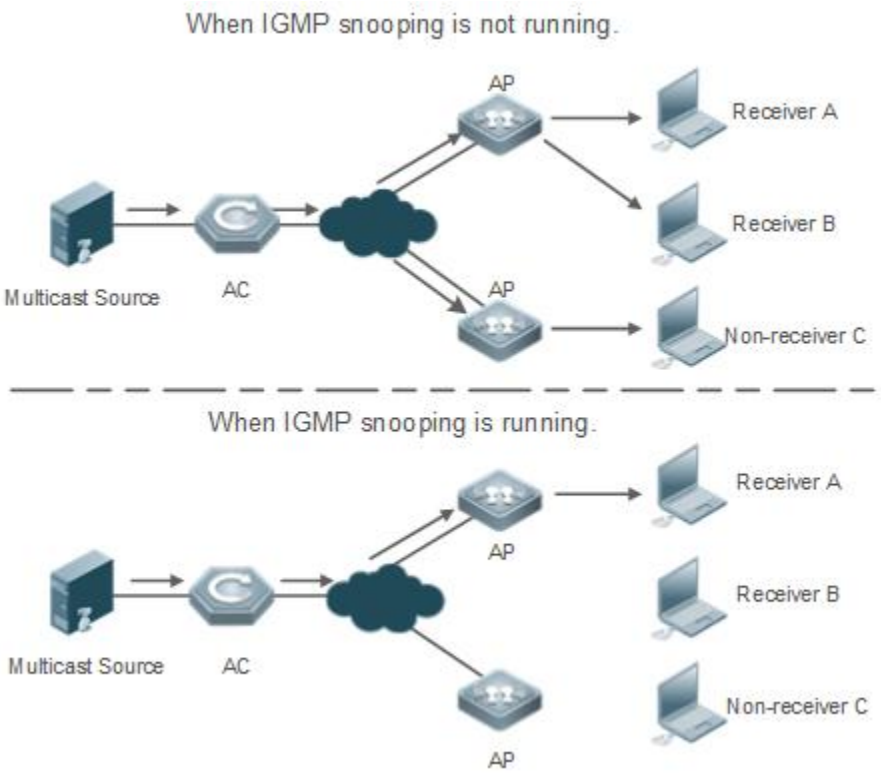
As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 13-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



As shown in the following figure, when IGMP Snooping does not run on the AC and AP in wireless multicast environment, multicast packets are broadcasted within the VLAN of the AC and are broadcasted by the AP to all wireless ports. When IGMP Snooping runs on both the AC and AP, multicast packets of a known multicast profile are not broadcasted but forwarded to specific receivers.

Figure 13-2 Forwarding of IP Multicast Streams in a VLAN Before and After IGMP Snooping Is Enabled on the AC and AP



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

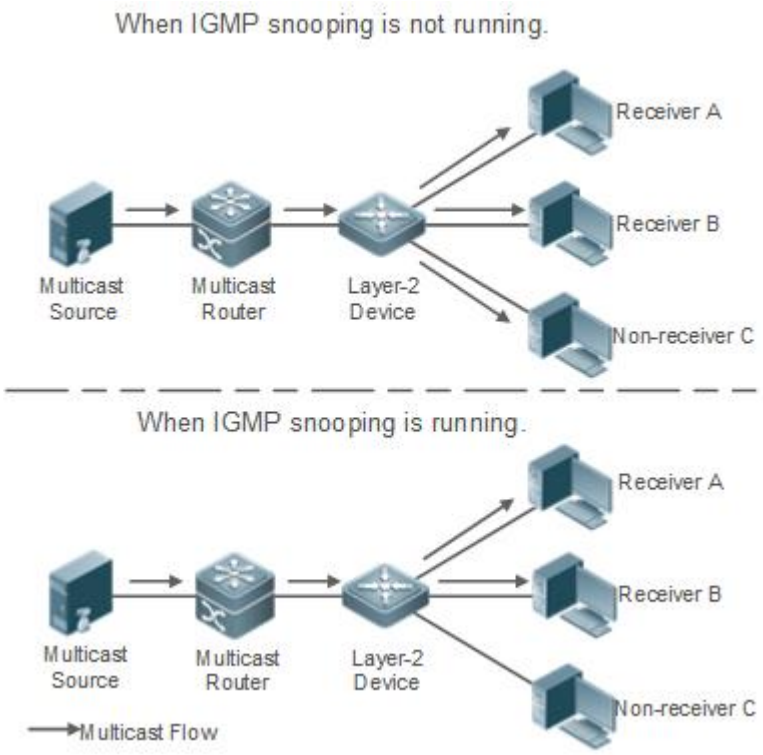
13.2 Applications

Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.

13.2.1 Layer-2 Multicast Control

Scenario

- As shown in the following figure, multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcast within the VLAN but transmitted to designated receivers.
- Figure 13-3 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



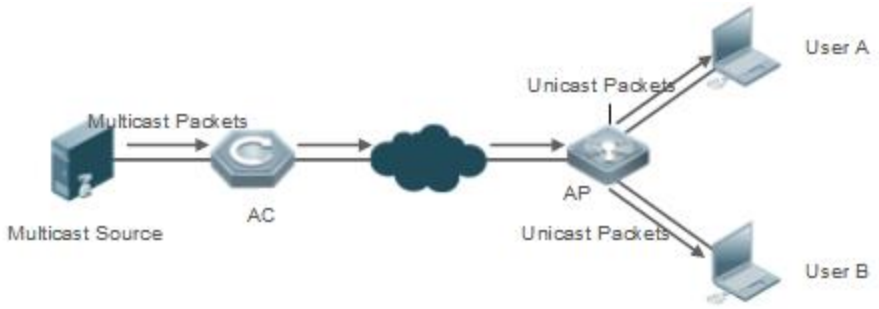
Deployment

- Configure basic IGMP snooping functions.

13.2.2 Multicast-to-Unicast Conversion

Scenario

- When multicast-to-unicast conversion is not configured, packets are transmitted from the AP to STAs in multicast mode. There is no acknowledgement and retransmission mechanism for multicast packets in wireless networks. As a result, severe packet loss occurs, which affect experience of wireless multicast services in video on demand and other applications. Wireless multicast packets between the AP and STAs can be configured to be transmitted in multicast-to-unicast conversion mode in order to reduce the packet loss rate and enhance user experience.
- Figure 13-4 Multicast-to-Unicast Conversion



Deployment

- Configure the multicast-to-unicast conversion function.

The function is available only in wireless multicast scenarios.

13.3 Features

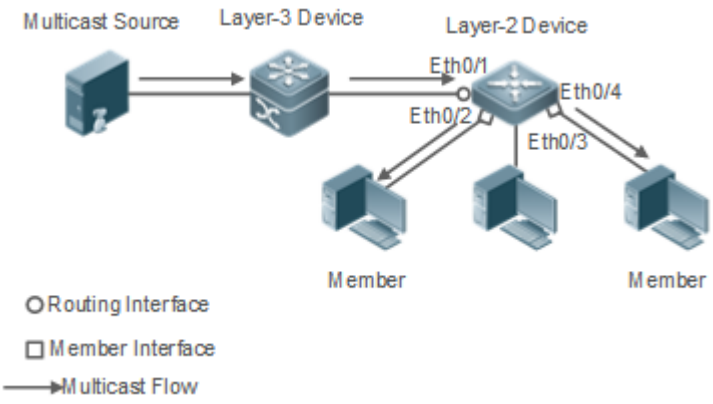
Basic Concepts

Multicast Router Ports and Member Ports

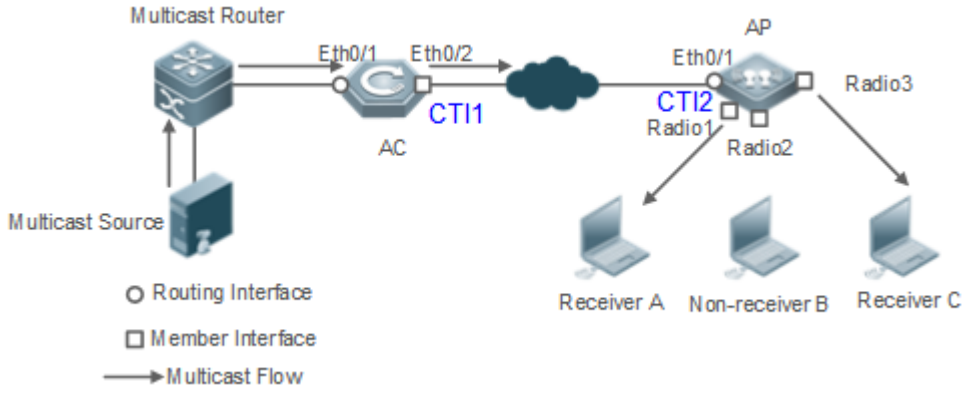
IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 13-5 Networking Topology of Two IGMP Snooping Ports



- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.
- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.
- Figure 13-6 Two Types of Ports in Wireless Environment



- Multicast router port: When the AC receives the PIM Hello or IGMP Query packet from the upstream multicast router (Layer-3 multicast device), the multicast router port Ethq/1 forms. When the AP receives the PIM Hello or IGMP Query packet forwarded by the AC, the multicast router port CTI2 also forms.
- Member port: also called listener port, that is, the port on a device for connecting to a multicast member. When Ports Radio1 and Radio3 on the AP receive Report packets from a wireless user receiver, they learn the wireless port as a member port. When the virtual interface CTI1 receives Report packets forwarded by the AP, it also learns the relevant wireless port as a member port.

IGMP Snooping Forwarding Entry

The device running IGMP snooping forwards IP multicast packets in accordance with the IGMP snooping forwarding entry.

An IGMP snooping forwarding entry includes the following items: source address (S), profile address (G), VLAN ID (VLAN_ID), multicast router port, and member port. It indicates that packets of required features (including S, G, and VLAN_ID) should enter the multicast router port and exit from a member port. An IGMP snooping forwarding entry is identified using a group of S, G, and VLAN_ID.

To display the IGMP snooping forwarding entry, run the **show ip igmp snooping gda-table** command.

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC  //Dynamic member port
  S: STATIC   //Static member port
  M: MROUTE   //Multicast router port (dynamic or static)
(*, 233.3.6.29, 1):   //(S: any; G: 233.3.6.29; VLAN_ID: VLAN 1)
  VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
    caPWAP-Tunnel 0/1(D)   // CAPWAP tunnel
(*, 233.3.6.30, 1):   //S: any; G: 233.3.6.30; VLAN_ID: VLAN 1)
  VLAN(1) 2 OPORTS:
GigabitEthernet 0/2(M)
GigabitEthernet 0/1(D)
```

```
(*,239.1.1.1, 1):  //(any source address, with the group address of 239.1.1.1 and VLAN ID of 1)
VLAN(1) 1 OPORTS:
    dot11radio 1/0.1 (D)  //wireless interface
```

Overview

Feature	Description
Listening to IGMP Packets	Discovers and identifies the router port and member port to establish and maintain the IGMP snooping forwarding entries. :
IGMP Snooping Working Modes	Provides independent or shared multicast services to the user VLAN.
IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.
Configuring Multicast-to-Unicast Conversion	Implements transmission of multicast packets between the AP and STAs in unicast mode.
Optimizing Multicast Wireless Environment Configuration	Ignores port timer resetting for query packets.

13.3.1 Listening to IGMP Packets

A device running IGMP snooping analyzes IGMP packets received, and finds and identifies the router port and member port using these packets, thereby creating and maintaining an IGMP snooping entry.

Working Principle

A device running IGMP snooping can identify and handle the following types of IGMP packets:

Query Packets

An IGMP querier periodically sends General Query packets. When the IGMP querier receives Leave packets, it sends Group-Specific Query packets.

When the device running IGMP snooping receives the Query packets, it performs the following operations within the VLAN:

- Forward the IGMP Query packets to all the ports (except the receiving port of these packets).
- If the receiving port is a dynamic router port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If the receiving port is not a dynamic router port, use it as a dynamic router port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- For general queries, reset the aging timer for all the dynamic member ports. If the timer expires, the port will no longer be used as the dynamic member port for the general group. By default, the maximum response time carried by the

IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.

- For designated query packets, reset the aging timer for all the dynamic member ports of the designated profile. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

Report Packets

When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.

By default, IGMP Snooping is capable of processing IGMPv1 and IGMPv2 packets. For IGMPv3 Report packets, it processes profile information but does not process carried source information. IGMP Snooping v3 can be configured to process all information in IGMPv1, IGMPv2, and IGMPv3 packets.

When the device running IGMP snooping receives the Report packets, it performs the following operations within the VLAN:

- Forward the Report packets from all the router ports. After the **ip igmp snooping suppression enable** command is run in one IGMP query cycle, only the first report received by each profile will be forwarded.
- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

Leave Packets

If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

Configuring the Aging Time of a Dynamic Router Port

The default aging time is 300s.

When a dynamic router port receives a query packet, the aging timer of the port is enabled or reset; if the aging time is not configured, the maximum response time carried by the query packet is used as the aging time.

Run **ip igmp snooping dyn-mr-aging-time** to configure the aging time of the dynamic router port.

Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a query packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time carried by the query packet.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

13.3.2 IGMP Snooping Working Modes

A device running in the IVGL mode of IGMP snooping can provide independent multicast services to the user VLAN.

Working Principle

IVGL

In IVGL mode, a device running IGMP snooping can provide independent multicast services to each user VLAN.

Independent multicast services indicate that multicast traffic can be forwarded only within the VLAN it belongs to, and a user host can subscribe to the multicast traffic within the VLAN that the host belongs to.

Related Configuration

Enabling IGMP Snooping and Selecting a Working Mode

IGMP snooping is disabled by default.

Run the **ip igmp snooping** command to enable IGMP snooping in IVGL mode.

13.3.3 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier. In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1, IGMPv2, or IGMPv3.

Configuring the Source IP Address of a Querier

You can configure the source IP address of a query packet sent by the querier based on VLANs.

When the source IP address of the querier is not configured, the querier will not take effect.

Configuring the Query Interval of a Querier

You can configure the intervals for sending global Query packets based on different queriers on different VLANs.

Configuring the Maximum Response Time of a Query Packet

You can configure the maximum response time carried by a Query packet that is sent by a querier. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1. You can configure different maximum response time for queriers on different VLANs.

Configuring the Aging Time of a Querier

When other IGMP queriers exist on a network, the existing device will compete with other queriers. If the existing device fails to be elected and is in the non-querier state, the aging timer of a querier will be enabled. After the timer expires, other queriers on the network are considered as expired and the existing device will be resumed as the querier.

Related Configuration

Enabling the Querier Function

By default, the querier function of a device is disabled.

Run the **ip igmp snooping querier** command to enable the global querier function.

Run the **ip igmp snooping vlan** *num* **querier** command to enable the querier function for specific VLANs.

Specifying the IGMP Version for a Querier

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

Configuring the Source IP Address of a Querier

By default, the source IP address of a querier is 0.

Run the ip igmp snooping querier address command to enable global source IP addresses of queriers.

Run the ip igmp snooping vlan querier address command to specify the source IP addresses of the queriers on specific VLANs.

Configuring the Query Interval of a Querier

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan querier query-interval** to specify the global query interval of the queriers on specific VLANs.

Configuring the Maximum Response Time of a Query Packet

By default, the maximum response time of a query packet is 10s.

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to configure the aging time of queriers on specific VLANs.

13.3.4 Multicast-to-Unicast Conversion

The multicast-to-unicast conversion function is available only in wireless environment. After the function is configured on a wireless device, multicast packets between an AP and STAs are transmitted in unicast mode. The multicast-to-unicast conversion function runs on the AP.

Working Principle

The following describes the working principle of multicast-to-unicast conversion from several scenarios in wireless environment.

In fat AP mode, IGMP Snooping needs to learn and track user information. After multicast-to-unicast conversion is configured, the wireless multicast fast forwarding module queries the users who need multicast-to-unicast conversion through the interface provided by the multicast-to-unicast conversion module, and replaces the destination MAC addresses in multicast packets of the users with the MAC addresses of STAs, and destination IP addresses with IP addresses of the STAs, and then forwards the multicast packets in unicast mode.

In fit AP centralized forwarding mode, an AC, according to recorded user information, queries the WLAN ID and RADIO ID of an STA for packets, conducts CAPWAP encapsulation on the packets, and then sends the packets to an AP. If the multicast-to-unicast conversion is enabled, packets sent to the AP are delivered to the wireless multicast fast forwarding module, which queries the interface of the multicast-to-unicast conversion module to learn about the users who need multicast-to-unicast conversion. Then, the AP transmits multicast packets in unicast mode.

In fit AP local forwarding mode, after packets are forwarded to an AP, if multicast-to-unicast conversion is enabled, the AP delivers the packets to the wireless multicast fast forwarding module, which transmit multicasts the packets in unicast mode.

Related Configuration

Enabling the Global Multicast Function

By default, the global multicast function is disabled. Run the **ip multicast wlan** command to enable the global multicast function. After global multicast is enabled, when an AC receives multicast packets, it conducts CAPWAP encapsulation on the multicast packets and sends the packets to the AP associated with the AC in CAPWAP unicast mode.

Run the **no ip multicast wlan** command to restore default configuration. After global multicast is disabled, an AC directly discards the received multicast packets.

Enabling Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is disabled.

In ap-config mode on an AC, run the **igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion, or on a fat AP, run the **ip igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion.

In ap-config mode on an AC, run the **no igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion, or on a fat AP, run the **no ip igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion.

Configuring the Multicast Range for Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is available to all multicast profiles.

Use AC as an example. In ap-config mode, run the **igmp snooping mcast-to-unicast group-range** command to configure the profile address range for multicast-to-unicast conversion.

In ap-config mode, run the **no igmp snooping mcast-to-unicast group-range** command to restore the default configuration.

Configuring the Maximum Number of Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion can be configured for a maximum of 64 multicast profiles.

Use AC as an example. In ap-config mode, run the **igmp snooping mcast-to-unicast max-group** command to configure the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.

In ap-config mode, run the **no igmp snooping mcast-to-unicast max-group** command to restore the default configuration.

13.3.5 Optimizing the Multicast Wireless Environment Configuration

Ignoring port timer resetting for query packets refers to not resetting the port aging timer when a device receives query packets.

When multiple STAs are configured in a congested wireless network, after an AP sends out a query packet, the IGMP report packet responded by STAs may be discarded or the STAs fail to receive the query packet, and as a result, the AP fails to receive responses from the STAs. Traffic interruption may occur on the STAs. In this case, this function can be configured, in combination with aging time configuration of member ports, to ensure that an STA does not age within multiple query intervals. If an IGMP report packet from the STA is received within the query intervals, the port timer time is reset as the port aging time.

The configuration takes effect when query packets are received next time. A port timer that has been reset on a port will not be cancelled. The configuration prolongs aging time. Use it in appropriate scenarios.

The function is disabled by default.

Use AC as an example. In ap-config mode, run the **igmp snooping ignore-query-timer** command to ignore the port aging timer resetting for query packets.

In ap-config mode, run the **no igmp snooping ignore-query-timer** command to restore the default configuration.

13.4 Configuration

Configuration	Description and Command	
Configuring Basic IGMP Snooping Functions (IVGL Mode)	⚠ Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode.	
	ip multicast wlan	Enables global multicast.
	ip igmp snooping	Enables global IGMP snooping on a Fat AP.
	igmp snooping	Enables global IGMP snooping on an AC.
	no ip igmp snooping vlan *num*	Disables IGMP snooping for a VLAN.
Configuring the Packet Processing	⚠ (Optional) It is used to adjust relevant configurations for processing protocol packets.	
	ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-id*	Configures a static router port.
	p igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	Configures a static member port.
	ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**	Enables dynamic router port learning.
	ip igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port on an AC.
	igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port on a Fat AP.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet on an AC.
	ip igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet on a Fat AP.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.

Configuring an IGMP Querier	(Optional) It is used to enable IGMP querier function on a network without a Layer-3 multicast device.	
	ip igmp snooping querier	Enables global querier function.
	ip igmp snooping vlan *num* **querier**	Enables the querier for a VLAN.
	ip igmp snooping querier version *num*	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan *num* **querier version** *num*	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address a.b.c.d	Configures the source IP address of queriers globally.
	ip igmp snooping vlan *num* **querier address** a.b.c.d	Configures the source IP address for a querier of a VLAN.
	ip igmp snooping querier query-interval *num*	Configures the query interval of queriers globally.
	ip igmp snooping vlan *num* **querier query-interval** *num*	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time *num*	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan *num* **querier max-response-time** *num*	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry *num*	Configures the aging timer for queriers globally.
	ip igmp snooping vlan *num* **querier timer expiry** *num*	Configures the aging timer for a querier of a VLAN.
Configuring Multicast-to-Unicast Conversion	**igmp snooping mcast-to-unicast enable**	Enables multicast-to-unicast conversion on an AC.
	ip igmp snooping mcast-to-unicast enable	Enables multicast-to-unicast conversion on an Fat AP.
	igmp snooping mcast-to-unicast group-range ***ip-addr ip-addr***	Configures an AP's maximum multicast range for multicast-to-unicast conversion on an AC.
	ip igmp snooping mcast-to-unicast group-range ***ip-addr ip-addr***	Configures an AP's maximum multicast range for multicast-to-unicast conversion on a Fat AP.
	igmp snooping mcast-to-unicast max-group ***group-num***	Configures an AP's maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion on an AC.

	ip igmp snooping mcast-to-unicast max-group *group-num*	Configures an AP's maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion on a Fat AP.
Opitimizing the Wireless Multicast Environment	**igmp snooping ignore-query-timer**	Configures the function of ignoring port aging timer resetting for query packets on n AC.
	ip igmp snooping ignore-query-timer	Configures the function of ignoring port aging timer resetting for query packets on a Fat AP.

13.4.1 Configuring Basic IGMP Snooping Functions (IVGL Mode)

Configuration Effect

- Enable IGMP snooping to realize Layer-2 multicast.
- Provide independent multicast services to each VLAN.

Configuration Steps

↘ Enabling Global Multicast

Mandatory.

After global multicast is enabled, IGMP snooping can be enabled.

↘ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

↘ Enabling Multicast of AP

Mandatory.

To enable multicast of AP, run the **igmp snooping** command in AP configuration mode of AC.

↘ Disabling IGMP Snooping for a VLAN

(Optional) You can use this function if you wish to disable IGMP snooping on specified VLANs.

Only when global IGMP snooping is enabled can it be disabled on specified VLANs.

In IVGL mode, each VLAN can enjoy independent multicast services. Disabling any VLAN multicast services will not interfere in the services provided to the others.

Verification

- Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table and verify that the member ports include only those connecting member hosts.

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL mode.

Related Commands

Enablingn Glocal Multicast

Command	**ip multicast wlan**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After global multicast is enabled, IGMP snooping can be enabled. By default, global multicast is disabled.

Enabling Global IGMP Snooping on a Fat AP

Command	**ip igmp snooping**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs. By default, IGMP snooping is disabled.

Enabling Global IGMP Snooping on an AC

Command	**igmp snooping**
Parameter Description	N/A
Command Mode	AP configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on the specified AP. By default, IGMP snooping is disabled.

Disabling IGMP Snooping for a VLAN

Command	**no ip igmp snooping vlan** *num*
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

Displaying the IGMP Snooping Entry

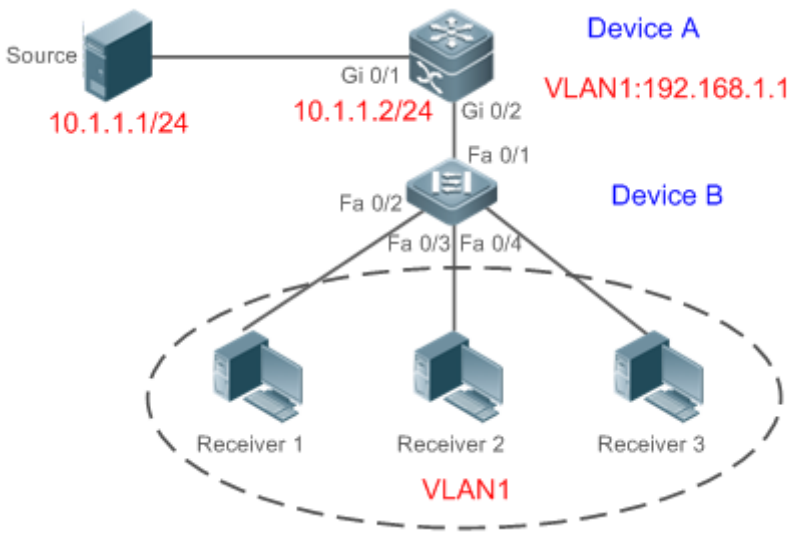
Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

Displaying the IGMP Snooping Working Mode

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: `IGMP Snooping running mode: IVGL`

Configuration Example

Providing Layer-2 Multicast Services for the Subnet Hosts

Scenario **Figure 13-7**	
	A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.
A	`A# configure terminal`

	A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)# ip igmp snooping ivgl
Verification	Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G. ● Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ● Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Fa0/2. ● Check whether the IGMP snooping working mode is IVGL.
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(1) 2 OPORTS: FastEthernet 0/1(M) FastEthernet 0/2(D) B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds) vlan 1 ---------- IGMP Snooping state: Enable

	Multicast router learning mode: pim-dvmrp IGMP Fast-Leave: Disabled IGMP VLAN querier: Disable IGMP VLAN Mode: STATIC

Common Errors

- The working mode of IGMP snooping is improper.

13.4.2 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.
- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network.
- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

↘ Configuring a Static Router Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

↘ Configuring a Static Member Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

↘ Enabling Report Packet Suppression

- Optional.

- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

Enabling the Immediate-Leave Function

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

Disabling Dynamic Router Port Learning

- Optional.
- This function is used when multicast traffic needs to be forwarded only within the Layer-2 topology but not to a Layer-3 router.

Configuring the Maximum Response Time of a Query Packet

- Optional.
- You can configure the aging time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

Configuring a Static Router Port

Command	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	In SVGL mode, if a sub VLAN is not configured, only the configurations for the static router port within the shared VLAN can take effect, and the others can be configured but cannot take effect. If a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL-SVGL mode, if a sub VLAN is not configured, the configurations for the static router ports within all the VLANs can take effect; if a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect.

	In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.

Configuring a Static Member Port

Command	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *group-address*: Indicates a profile address. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

Enabling Report Packet Suppression

Command	**ip igmp snooping suppression enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

Enabling the Immediate-Leave Function

Command	**ip igmp snooping fast-leave enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address. The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.

Enabling Dynamic Router Port Learning

Command	**ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command	Global configuration mode

Mode	
Usage Guide	A router port is the port that is connected directly to a multicast device running IGMP snooping and a multicast neighbor device running multicast routing protocol. By default, dynamic router port learning is enabled and the device automatically listens to IGMP Query packets, DVMRP packets, and PIM Hello packets.

Configuring the Aging Time of a Dynamic Member Port

Command	**ip igmp snooping host-aging-time** *seconds*
Parameter Description	*seconds*: Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile. When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.

Configuring the Maximum Response Time of a Query Packet

Command	**ip igmp snooping query-max-response-time** *seconds*
Parameter Description	*seconds*: Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. When an IGMP profile-specific Query packet is received, the multicast device will reset the aging time of all the dynamic member ports of the specific profile, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. This configuration takes effect after the next Query packet is received, and the timer in use will not be refreshed. The timer of an IGMPv3 profile-specific Query packet is not refreshed.

Displaying Router Ports

Command	**show ip igmp snooping mroute**
Parameter	N/A

Description	
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the router port is successfully configured, an "S" will be displayed in the port information. `Ruijie(config)#show ip igmp snooping mrouter` `Multicast Switching Mroute Port` `  D: DYNAMIC` `  S: STATIC` `(*, *, 1):` `  VLAN(1)  1 MROUTES:` `    GigabitEthernet 0/1(S)`

Displaying the Information of Dynamic Router Port Learning

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time and learning status of the dynamic router port. `Dynamic Mroute Aging Time : 300(Seconds)` `Multicast router learning mode: pim-dvmrp`

Displaying the Information of a Member Port

Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the member port is successfully configured, an "S" will be displayed in the port information. `Ruijie(config)#show ip igmp snooping gda-table` `Multicast Switching Cache Table` `  D: DYNAMIC` `  S: STATIC` `  M: MROUTE` `(*, 224.1.1.1, 1):` `  VLAN(1) 1 OPORTS:` `    GigabitEthernet 0/1(S`

Displaying Other Parameters

Command	**show ip igmp snooping**

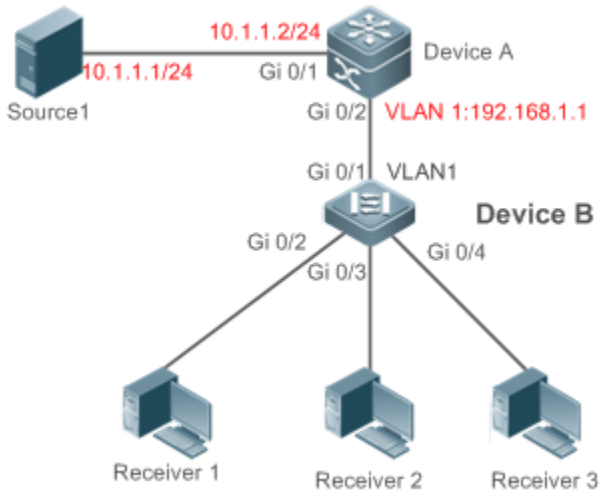
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show ip igmp snooping** command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave. `IGMP Fast-Leave: Enable` `IGMP Report suppress: Enable` `Query Max Response Time: 20(Seconds)` `Dynamic Mroute Aging Time : 300(Seconds)` `Dynamic Host Aging Time : 260(Seconds)`

Configuration Example

Configuring a Static Router Port and Static Member Port

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	`Ruijie# configure terminal` `Ruijie(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0` `Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0` `Ruijie(config)# end`
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.
	`Ruijie#show ip igmp snooping mrouter` `Multicast Switching Mroute Port` `  D: DYNAMIC` `  S: STATIC` `(*, *, 1):` `  VLAN(1)  1 MROUTES:` `GigabitEthernet 0/0(S)` `Ruijie#show ip igmp snooping gda-table` `Multicast Switching Cache Table` `  D: DYNAMIC` `  S: STATIC` `  M: MROUTE` `(*, 224.1.1.1, 1):` `  VLAN(1) 1 OPORTS:` `  GigabitEthernet 0/0(SM)`

Enabling Report Packet Suppression

Scenario **Figure 13-8**	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode. ● Enable Report packets suppression on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable
Verification	Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.
B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable

	IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Configuring Other Parameters

Configuration Steps	• Configure basic IGMP snooping functions. • Enable Immediate-leave function. • Disable router port learning. • Configure the aging time of a router port. • Configuring the aging time of a member port. • Configure the response time of a Query packet.
	Ruijie# configure terminal Ruijie(config)# ip igmp snooping fast-leave enable Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp Ruijie(config)#ip igmp snooping dyn-mr-aging-time 200 Ruijie(config)#ip igmp snooping host-aging-time 100 Ruijie(config)#ip igmp snooping query-max-response-time 60 Ruijie(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.
	Ruijie#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Host Aging Time : 100(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

13.4.3 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

Enabling the Querier Function

- (Optional) Enable IGMP querier function globally or for a specified VLAN.
- (Optional) Disable the IGMP querier function for a specified VLAN.

Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.

Configuring the Maximum Response Time of a Query Packet

- (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.

Configuring the Query Interval of a Querier

- (Optional) Adjust the interval of the IGMP querier for sending query packets.

Configuring the Aging Timer of a Querier

- (Optional) Configure the aging timer of other IGMP queriers on the network.

Specifying the IGMP Version for a Querier

- (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

Enabling the IGMP Querier Function

Command	**ip igmp snooping** [**vlan** *vid*] **querier**

Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

Configuring the Source IP Address of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *a.b.c.d*: Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

Configuring the Maximum Response Time of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Query Interval of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

Configuring the Aging Timer of a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *seconds*: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails

	to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

Specifying the IGMP Version for a Querier

Command	**ip igmp snooping** [**vlan** *vid*] **querier version 1**
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

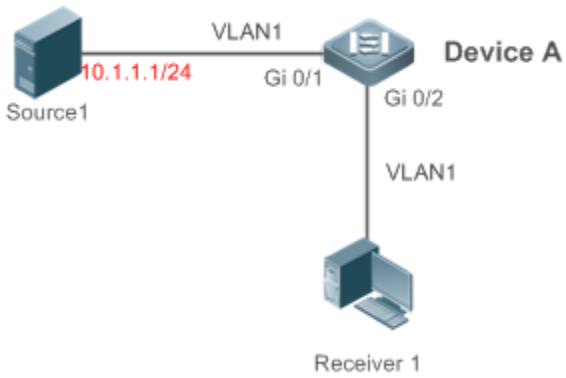
Displaying the IGMP Querier Configuration

Command	**show ip igmp snooping querier detail**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. `Ruijie(config)#show ip igmp snooping querier detail` `Vlan IP Address IGMP Version Port` `----------` `Global IGMP switch querier status` `----------` `admin state : Enable` `admin version : 2` `source IP address : 1.1.1.1` `query-interval (sec) : 60` `max-response-time (sec) : 10` `querier-timeout (sec) : 125` `Vlan 1: IGMP switch querier status` `----------` `admin state : Disable` `admin version : 2` `source IP address : 1.1.1.1` `query-interval (sec) : 60` `max-response-time (sec) : 10`

	querier-timeout (sec) : 125 operational state : Disable operational version : 2

Configuration Example

Enabling the IGMP Querier Function

Scenario **Figure 13-9**	
	In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.
Configuration Steps	● Enable global IGMP snooping on A in IVGL mode. ● Enable IGMP querier for VLAN 1 on A.
A	A(config)#ip igmp snooping ivgl A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier
Verification	Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.
A	A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port --- 1 10.1.1.1 2 switch A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier status --- elected querier is 10.1.1.1 (this switch querier) --- admin state : Enable

```
admin version                : 2
source IP address            : 10.1.1.1
query-interval (sec)         : 60
max-response-time (sec)      : 10
querier-timeout (sec)        : 125
operational state            : Querier
operational version          : 2
```

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

13.4.4 Configuring Multicast-to-Unicast Conversion

Configuration Effect

- Enable the multicast-to-unicast conversion on the AP, which transmits multicast packets to STAs in unicast mode.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

Enabling Global Multicast

- (Mandatory) Enable global multicast in global mode.
- If global multicast is disabled in global mode, a wireless device directly discards received packets.

Enabling Multicast-to-Unicast Conversion

- (Optional) Configure whether to enable multicast-to-unicast conversion. After multicast-to-unicast conversion is enabled, after packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode and transmits such packets in unicast mode.

Configuring the Multicast Range for Multicast-to-Unicast Conversion

- (Optional) Multicast-to-unicast conversion is available to all multicast groups by default. A multicast range can be configured to allow multicast packets to be transmitted in unicast mode, so as to utilize AP resources to the maximum extent.

Configuring the Maximum Number of Multicast Profiles that Are Allowed to Use Multicast-to-Unicast Conversion

- (Optional) The maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion can be adjusted.
- It is used in combination with the multicast range of multicast-to-unicast conversion.

Verification

- Run the show ip igmp snooping command to check whether the configuration takes effect.

Related Commands

Configuring Global Multicast

Command	**ip multicast wlan**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	If global multicast is enabled, multicast packets are processed only after they reach the AC. If global multicast is disabled, the AC directly discards the received multicast packets.

Configuring Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast enable**
Parameter Description	N/A
Command Mode	ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	After multicast-to-unicast conversion is enabled, when multicast packets reach the AP, the AP judges the multicast packets that need to be transmitted in unicast mode according to the multicast-to-unicast conversion policy.

Configuring the Maximum Multicast Range for Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast group-range** *ip-addr ip-addr*
Parameter Description	*ip-addr:* Indicates the multicast profile range. The value must be valid multicast addresses and ranges from 224.0.1.0 to 239.255.255.255.
Command Mode	Ap-config mode on the AC or global configuration mode on the fat AP
Usage Guide	If the multicast range of multicast-to-unicast conversion is not configured, multicast-to-unicast conversion is available to all multicast profiles by default.

Configuring the Maximum Number of Multicast Profiles That Are Allowed to Use Multicast-to-Unicast Conversion

Command	**igmp snooping mcast-to-unicast max-group** *number*
Parameter Description	number: Indicates the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion. The value ranges from 1 to 64. The default value is 64.
Command Mode	ap-config mode on the AC or global configuration mode on the fat AP

Usage Guide	It can be used in combination with the maximum multicast range of multicast-to-unicast conversion so as to properly allocate bandwidth and effectively control AP resources.

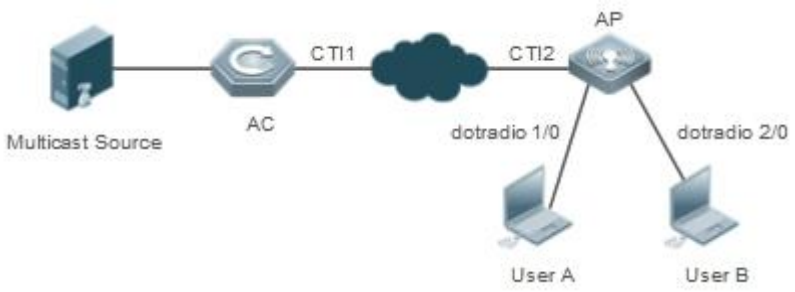
Displaying Multicast-to-Unicast Conversion Configuration

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	If multicast-to-unicast conversion is configured successfully, the following information is displayed: `Ruijie(config)#sh ip igmp snooping` `WLAN Multicast: Enable` `IGMP Snooping running mode: IVGL` `IGMP Snooping M2U-Forward: Enable` `IGMP Snooping Support M2U Max-Group Num: 64` `IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64` `IGMP Snooping L2-entry-limit: 65536` `Source port check: Disable` `Source ip check: Disable` `IGMP Fast-Leave: Disable` `IGMP Report suppress: Disable` `IGMP Global Querier: Disable` `IGMP Preview: Disable` `IGMP Tunnel: Disable` `IGMP Preview group aging time : 60(Seconds)` `Dynamic Mroute Aging Time : 300(Seconds)` `Dynamic Host Aging Time : 260(Seconds)`

Configuration Example

The following configuration example describes only configurations related to IGMP Snooping.

Enabling the IGMP Querier

Scenario **Figure 13-10**	

	Multicast streams only need to be forwarded at Layer 2 in network deployment and there is no device supporting the Layer-3 multicast function in the network. User A and User B are multicast receivers.
Configuration Steps	● Enable IGMP Snooping on the AC. ● Enable global multicast on the AC. ● Enable IGMP Snooping in ap-config mode. ● Enable multicast-to-unicast conversion in ap-config mode. ● Configure the maximum multicast range for multicast-to-unicast conversion in ap-config mode. ● Configure the maximum number of multicast profiles that are allowed to support multicast-to-unicast conversion in ap-config mode.
A	A(config)#ip igmp snooping ivgl A(config)#ip multicast wlan A(config)#ap-confing all A(config-ap)#igmp snooping A(config)#igmp snooping mcast-to-unicast enable A(config-ap)#igmp snooping mcast-to-unicast group-range 233.1.1.1 233.255.255.255 A(config-ap)#igmp snooping mcast-to-unicast max-group 10
Verification	Run the **show ip igmp snooping** command to check whether the configuration takes effect.
A	A(config)# sh ip igmp snooping WLAN Multicast: Enable IGMP Snooping running mode: IVGL IGMP Snooping M2U-Forward: Enable IGMP Snooping Support M2U Max-Group Num: 64 IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64 IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

Common Errors

- Multicast packets are not processed because global multicast is not configured.

13.4.5 Optimizing the Wireless Multicast Environment

Configuration Effect

- Configure the function of ignoring port timer resetting for query packets on the wireless device.

Notes

- IGMP Snooping basic functions must be configured.

Configuration Steps

↘ **Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets**

- (Optional) Configure the function of ignoring port aging timer resetting for query packets so that the port does not age within multiple query intervals.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

↘ **Configuring the Function of Ignoring Port Aging Timer Resetting for Query Packets**

Command	**Ip igmp snooping ignore-query-timer**
Parameter Description	N/A
Command Mode	Global configuration mode or ap-config mode
Usage Guide	After the function of ignoring port aging timer for query packets is configured, the port does not age within multiple query intervals. When the port receives a Report request, the port aging timer resets.

13.5 Monitoring

Clearing

⚠ Running the **clear** commands may lose vital information and thus interrupt services.

Description	**Command**
Clears the dynamic router ports and member ports.	**clear ip igmp snooping gda-table**

Displaying

Description	**Command**

Displays basic IGMP snooping configurations.	**show ip igmp snooping** [**vlan** *vlan-id*]
Displays the router ports.	**show ip igmp snooping mrouter**
Displays the IGMP snooping entries.	**show ip igmp snooping gda-table**
Displays the IGMP querier.	**show ip igmp snooping querier** [**detail**]
Displays user information.	**show ip igmp snooping user-info**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all IGMP Snooping functions.	**debug igmp-snp**
Debugs the IGMP snooping events.	**debug igmp-snp event**
Debugs the IGMP snooping packets.	**debug igmp-snp packet**
Debugs the communications between IGMP snooping and MSF.	**debug igmp-snp msf**
Debugs the IGMP snooping alarms.	**debug igmp-snp warning**

14 Configuring the ACL

14.1 Overview

Access control list (ACL) is also called access list or firewall. It is even called packet filtering in some documents. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

ACLs are classified by function into two types:

- Security ACLs: Used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: Used to classify and process data flows by priority.

ACLs are configured for a lot of reasons. Major reasons include:

- Network access control: To ensure network security, rules are defined to limit access of users to some services (for example, only access to the WWW and email services is permitted, and access to other services such as Telnet is prohibited), or to allow users to access services in a specified period of time, or to allow only specified hosts to access the network.
- QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about the use of QoS ALCs, see the configuration manual related to QoS.

14.2 Applications

Application	Description
Access Control of an Enterprise Network	On an enterprise network, the network access rights of each department, for example, access rights of servers and use permissions of chatting tools (such as QQ and MSN), must be controlled according to requirements.

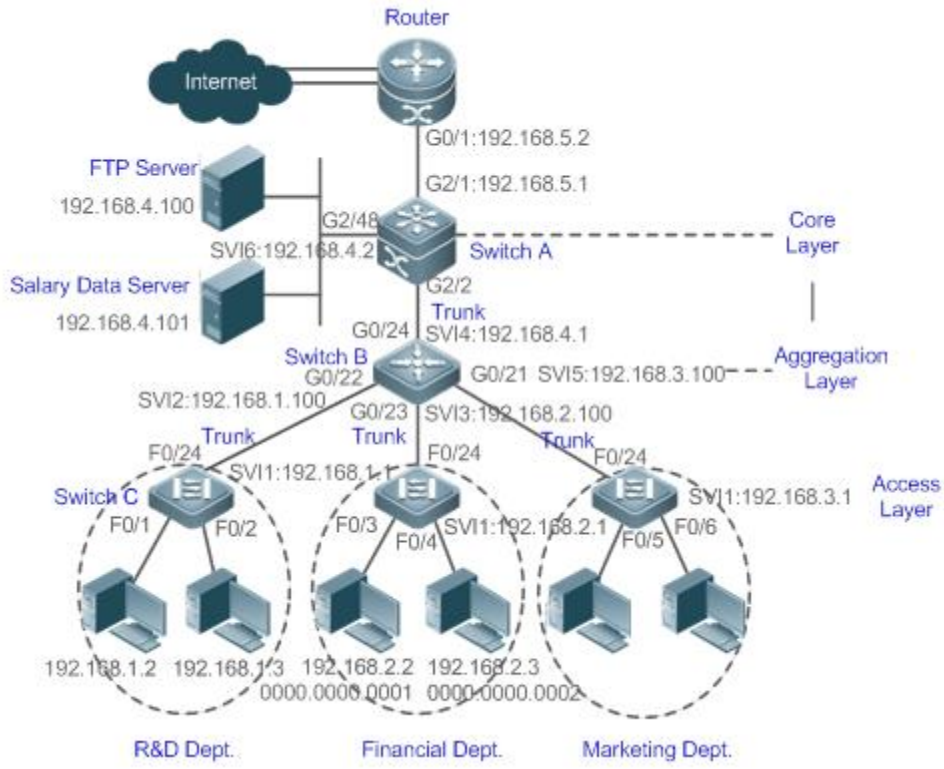
14.2.1 Access Control of an Enterprise Network

Scenario

Internet viruses can be found everywhere. Therefore, it is necessary to block ports that are often used by viruses to ensure security of an enterprise network as follows:

- Allow only internal PCs to access the server.
- Prohibit PCs of a non-financial department from accessing PCs of the financial department, and prohibit PCs of a non-R&D department from accessing PCs of the R&D department.
- Prohibit the staff of the R&D department from using chatting tools (such as QQ and MSN) during working hours from 09:00 to 18:00.

Figure 14-1



Remarks	Switch C at the access layer:It is connected to PCs of each department and to Switch B at the aggregation layer through the gigabit optical fiber (trunk mode). Switch B at the aggregation layer:Multiple virtual local area networks (VLANs) are divided. One VLAN is defined for one department. These VLANs are connected to Switch A at the core layer through the 10-gigabit optical fiber (trunk mode). Switch A at the core layer:It is connected to various servers, such as the File Transfer Protocol (FTP) server and Hypertext Transfer Protocol (HTTP) server, and to the Internet through firewalls.

Deployment

- Configure an extended ACL on the port G2/1 to filter data packets, thus protecting the network against the viruses. This port is located on a core-layer device (Switch A) and used to connect Switch A to the uplink port G2/1 of a router.
- Allow only internal PCs to access servers, and prohibit external PCs from accessing servers. Define and apply the extended IP ACLs on G2/2 or switch virtual interface (SVI) 2 that is used to connect Switch A to an aggregation layer device or server.
- Prohibit mutual access between specified departments. Define and apply the extended IP ACLs on G0/22 and G0/23 of Switch B.
- Configure and apply the time-based extended IP ACLs on SVI 2 of Switch B to prohibit the R&D department from using chatting tools (such as QQ and MSN) in a specified period of time.

14.3 Features

Basic Concepts

ACL

ACLs include basic ACLs and dynamic ACLs.

You can select basic or dynamic ACLs as required. Generally, basic ACLs can meet the security requirements. However, experienced hackers may use certain software to access the network by means of IP address spoofing. If dynamic ACLs are used, users are requested to pass identify authentication before accessing the network, which prevents hackers from intruding the network. Therefore, you can use dynamic ACLs in some sensitive areas to guarantee network security.

IP address spoofing is an inherent problem of all ACLs, including dynamic ACLs. Hackers may use forged IP addresses to access the network during the validity period of authenticated user identities. Two methods are available to resolve this problem. One is to set the idle time of user access to a smaller value, which increases the difficulty in intruding networks. The other is to encrypt network data using the IPSec protocol, which ensures that all data is encrypted when arriving at a device.

ACLs are generally configured on the following network devices:

- Devices between the internal network and the external network (such as the Internet)
- Devices on the border of two network segments
- Devices connected to controlled ports

ACL statements must be executed in strict compliance with their sequence in the ACL. Comparison starts from the first statement. Once the header of a data packet matches a statement in the ACL, the subsequent statements are ignored and no longer checked.

Input/Output ACLs, Filtering Field Template, and Rules

When receiving a packet on an interface, the device checks whether the packet matches any access control entry (ACE) in the input ACL of this interface. Before sending a packet through a interface, the device checks whether the packet matches any ACE in the output ACL of this interface.

When different filtering rules are defined, all or only some rules may be applied simultaneously. If a packet matches an ACE, this packet is processed according to the action policy (permit or deny) defined in this ACE. ACEs in an ACL identify Ethernet packets based on the following fields in the Ethernet packets:

Layer 2 (L2) fields:

- 48-bit source MAC address (containing all 48 bits)
- 48-bit destination MAC address (containing all 48 bits)
- 16-bit L2 type field

Layer 3 (L3) fields:

- Source IP address field (All source IP address values can be specified, or the subnet can be used to define a type of data flows.)
- Destination IP address field (All destination IP address values can be specified, or the subnet can be used to define a type of data flows.)
- Protocol type field

Layer 4 (L4) fields:

- Either a TCP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.
- Either a UDP source or destination port is specified, or both are specified, or the range of the source or destination port is specified.

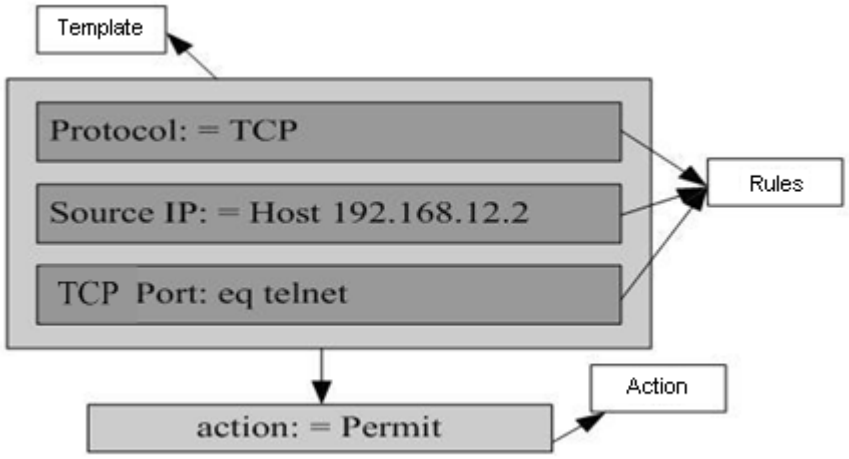
Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

Rules refer to values of fields in the filtering field template of an ACE.For example, the content of an ACE is as follows:

permit tcp host *192.168.12.2* any eq telnet

In this ACE, the filtering field template is a combination of the following fields:source IP address field, IP protocol field, and TCP destination port field. The corresponding values (rules) are as follows:source IP address = Host 192.168.12.2; IP protocol = TCP; TCP destination port = Telnet.

Figure 14-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



A filtering field template can be a combination of L3 and L4 fields, or a combination of multiple L2 fields. The filtering field template of a standard or an extended ACL, however, cannot be a combination of L2 and L3 fields, a combination

of L2 and L4 fields, or a combination of L2, L3, and L4 fields. To use a combination of L2,L3, and L4 fields, you can use the expert ACLs.

- An SVI associated with ACLs in the outgoing direction supports the IP standard, IP extended, MAC extended, and expert ACLs.
- If an expert ACL is configured and applied to the outgoing direction of an interface, and some ACEs in this ACL contain the L3 matching information (e.g. the IP address and L4 port), non-IP packets sent to the device from this interface cannot be controlled by the permit and deny ACEs in this ACL.
- If ACEs of an ACL (IP ACL or expert extended ACL) are configured to match non-L2 fields (such as SIP and DIP), the ACL does not take effect on tagged MPLS packets.

Overview

Feature	Description
IP ACL	Control incoming or outgoing IPv4 packets of a device based on the L3 or L4 information in the IPv4 packet header.
MAC Extended ACL	Control incoming or outgoing L2 packets of a device based on the L2 information in the Ethernet packet header.
Expert Extended ACL	Combine the IP ACL and MAC extended ACL into an expert extended ACL, which controls (permits or denies) incoming or outgoing packets of a device using the same rule based on the L2, L3, and L4 information in the packet header.
IPv6 ACL	Control incoming or outgoing IPv6 packets of a device based on the L3 or L4 information in the IPv6 packet header.
Security Channel	Allow packets to bypass the check of access control applications, such as DOT1X and Web authentication, to meet requirements of some special scenarios.
SVI Router ACL	Enable users in the same VLAN to communicate with each other.

14.3.1 IP ACL

The IP ACL implements refined control on incoming and outgoing IPv4 packets of a device. You can permit or deny the entry of specific IPv4 packets to a network according to actual requirements to control access of IP users to network resources.

Working Principle

Define a series of IP access rules in the IP ACL, and then apply the IP ACL either in the incoming or outgoing direction of an interface or globally. The device checks whether the incoming or outgoing IPv4 packets match the rules and accordingly forwards or blocks these packets.

To configure an IP ACL, you must specify a unique name or ID for the ACL of a protocol so that the protocol can uniquely identify each ACL. The following table lists the protocols that can use IDs to identify ACLs and the range of IDs.

Protocol	ID Range
Standard IP	1–99, 1300–1999
Extended IP	100–199, 2000–2699

Basic ACLs include the standard IP ACLs and extended IP ACLs. Typical rules defined in an ACL contain the following matching fields:

- Source IP address
- Destination IP address
- IP protocol number
- L4 source port ID or ICMP type
- L4 destination port ID or ICMP code

The standard IP ACL (ID range: 1–99, 1300–1999) is used to forward or block packets based on the source IP address, whereas the extended IP ACL (ID range: 100–199, 2000–2699) is used to forward or block packets based on a combination of the preceding matching fields.

For an individual ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

For routing products, the ICMP code matching field in an ACL rule is ineffective for ICPM packets whose ICPM type is 3. If the ICPM code of ICMP packets to be matched is configured in an ACL rule, the ACL matching result of incoming ICMP packets of a device whose ICPM type is 3 may be different from the expected result.

Implicit "Deny All Traffic" Rule Statement

At the end of every IP ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL permits only packets sent from the source host 192.168.4.12, and denies packets sent from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 1 deny any**.

If the ACL contains only the following statement:

```
access-list 1 deny host 192.168.4.12
```

Packets sent from any host will be denied when passing through this port.

When defining an ACL, you must consider the routing update packets. As the implicit "deny all traffic" statement exists at the end of an ACL, all routing update packets may be blocked.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and denies all traffic, all subsequent statements will not be checked.

For example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eqtelnetany
```

The first rule statement denies all IP packets. Therefore, Telnet packets from the host on the network 192.168.12.0/24 will be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

Configuring an IP ACL

By default, no IP ACL is configured on a device.

Run the **ip access-list { standard | extended } {*acl-name* | *acl-id*}** command in global configuration mode to create a standard or an extended IP ACL and enter standard or extended IP ACL mode.

Adding ACEs to an IP ACL

By default, a newly created IP ACL contains an implicit ACE that denies all IPv4 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv4 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv4 packets, add some ACEs to the ACL.

For a standard IP ACL, add ACEs as follows:

- No matter whether the standard IP ACL is a named or number ACL, you can run the following command in standard IP ACL mode to add an ACE:
  [*sn*] { **permit** | **deny** } {**host***source*| **any** | *sourcesource-wildcard* } [**time-range***time-range-name*]
- For a numbered standard IP ACL, you can also run the following command in global configuration mode to add an ACE:
  access-list *acl-id* { **permit** | **deny** } {**host***source*| **any** | *sourcesource-wildcard* } [**time-range***tm-rng-name*]

For an extended IP ACL, you can add ACEs as follows:

- No matter whether the extended IP ACL is a named or numbered ACL, you can run the following command in extended IP ACL mode to add an ACE:
  [*sn*] { **permit** | **deny** } *protocol*{**host***source*| **any** | *sourcesource-wildcard* } {**host***destination* | **any** | *destination destination-wildcard* }[[**precedence***precedence* [**tos** *tos]*] | **dscp***dscp*] [**fragment**] [**time-range***time-range-name*]
- For a numbered extended IP ACL, you can also run the following command in global configuration mode to add an ACE:
  access-list *acl-id* { **permit** | **deny** } *protocol*{**host***source*| **any** | *sourcesource-wildcard* } {**host***destination* | **any** | *destination destination-wildcard* }[[**precedence***precedence* [**tos** *tos]*] | **dscp***dscp*] [**fragment**]
  [**time-range***time-range-name*]

Applying an IP ACL

By default, the IP ACL is not applied to any interface/VXLAN, that is, the IP ACL does not filter incoming or outgoing IP packets of the device.

Run the **ip access-group { *acl-id* | *acl-name* } { in| out }[reflect]** command in interface/VXLAN configuration mode to apply a standard or an extended IP ACL to a specified interface/VXLAN. By default, a reflexive ACL is disabled on a router. You can run the **reflect** command to enable the reflexive ACL. The working principle of the reflexive ACL is as follows:

a. A temporary ACL is automatically generated based on the L3 and L4 information of the traffic originated by the internal network. The temporary ACL is created according to the following principles: The IP protocol number remains unchanged, the source and destination IP addresses are swapped, and the TCP/UDP source and destination ports are also swapped.

b. The router allows traffic to enter the internal network only when the L3 and L4 information of the returned traffic exactly matches that of the temporary ACL previously created based on the outgoing traffic.

14.3.2 MAC Extended ACL

The MAC extended ACL implements refined control on incoming and outgoing packets based on the L2 header of packets. You can permit or deny the entry of specific L2 packets to a network, thus protecting network resources against attacks or control users' access to network resources.

Working Principle

Define a series of MAC access rules in the MAC extended ACL, and then apply the ACL to the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an MAC extended ACL, you must specify a unique name or ID for this ACL to uniquely identify the ACL. The following table lists the range of IDs that identify MAC extended ACLs.

Protocol	ID Range
MAC extended ACL	700–799

Typical rules defined in an MAC extended ACL include:

- Source MAC address
- Destination MAC address
- Ethernet protocol type

The MAC extended ACL (ID range: 700–799) is used to filter packets based on the source or destination MAC address and the Ethernet type in the packets.

For an individual MAC extended ACL, multiple independent ACL statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL. However, more statements mean that it is increasingly difficult to read and understand the ACL.

If ACEs in an MAC extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the MAC extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

Implicit "Deny All Traffic" Rule Statement

At the end of every MAC extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only packets from the host with the MAC address 00d0.f800.0001, and denies packets from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 700 deny any any**.

Related Configuration

Configuring an MAC Extended ACL

By default, no MAC extended ACL is configured on a device.

Run the **mac access-list extended {*acl-name* | *acl-id* }** command in global configuration mode to create an MAC extended ACL and enter MAC extended ACL mode.

Adding ACEs to an MAC Extended ACL

By default, a newly created MAC extended ACL contains an implicit ACE that denies all L2 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an MAC extended ACL as follows:

- No matter whether the MAC extended ACL is a named or numbered ACL, you can run the following command in MAC extended ACL mode to add an ACE:
  [*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr* }{**any** | **host** *dst-mac-addr* } [*ethernet-type*] [**cos***cos*] [**inner***cos*] [**time-range***tm-rng-name*]
- For a numbered MAC extended ACL, you can also run the following command in global configuration mode to add an ACE:
  access-list *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr* }{**any** | **host** *dst-mac-addr* } [*ethernet-type*] [**cos***cos*] [**inner***cos*] [**time-range***time-range-name*]

Applying an MAC Extended ACL

By default, the MAC extended ACL is not applied to any interface, that is, the created MAC extended ACL does not filter incoming or outgoing L2 packets of a device.

Run the **mac access-group { *acl-id* | *acl-name* } { in| out }** command in interface/VXLAN configuration mode to apply an MAC extended ACL to a specified interface/VXLAN.

14.3.3 Expert Extended ACL

You can create an expert extended ACL to match the L2 and L3 information in packets using the same rule. The expert extended ACL can be treated as a combination and enhancement of the IP ACL and the MAC extended ACL because the expert extended ACL can contain ACEs in both the IP ACL and the MAC extended ACL. In addition, the VLAN ID can be specified in the expert extended ACL to filter packets.

Working Principle

Define a series of access rules in the expert extended ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an expert extended ACL, you must specify a unique name or ID for this ACL so that the protocol can uniquely identify each ACL. The following table lists the ID range of the expert extended ACL.

Protocol	ID Range
Expert extended ACL	2700–2899

When an expert extended ACL is created, defined rules can be applied to all packets. The device determines whether to forward or block packets by checking whether packets match these rules.

Typical rules defined in an expert extended ACL include:

- All information in the basic ACL and MAC extended ACL
- VLAN ID

The expert extended ACL (ID range: 2700–2899) is a combination of the basic ACL and MAC extended ACL, and can filter packets based on the VLAN ID.

For an individual expert extended ACL, multiple independent statements can be used to define multiple rules. All statements reference the same ID or name so that these statements are bound with the same ACL.

If rules in an expert extended ACL are not defined specifically for IPv6 packets, that is, the Ethernet type is not specified or the value of the Ethernet type field is not 0x86dd, the expert extended ACL does not filter IPv6 packets. If you want to filter IPv6 packets, use the IPv6 extended ACL.

Implicit "Deny All Traffic" Rule Statement

At the end of every expert extended ACL is an implicit "deny all traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
access-list 2700permit 0x0806 any any any any any
```

This ACL permits only ARP packets whose Ethernet type is 0x0806, and denies all other types of packets. This is because the following statement exists at the end of this ACL: **access-list 2700 deny any any any any**.

Related Configuration

Configuring an Expert Extended ACL

By default, no expert extended ACL is configured on a device.

Run the **expert access-list extended {*acl-name* | *acl-id* }** command in global configuration mode to create an expert extended ACL and enter expert extended ACL mode.

Adding ACEs to an Expert Extended ACL

By default, a newly created expert extended ACL contains an implicit ACE that denies all packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all L2 packets will be discarded. Therefore, if you want the device to receive or send some specific L2 packets, add some ACEs to the ACL.

You can add ACEs to an expert extended ACL as follows:

- No matter whether the expert extended ACL is a named or numbered ACL, you can run the following command in expert extended ACL mode to add an ACE:

  [*sn*] { **permit** | **deny** } [*protocol*| [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[[VID** [*out*] **[inner** *in*]]] { *sourcesource-wildcard* | **host***source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host***destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence***precedence*] [**tos** *tos*] [**fragment**] [**range***lowerupper*] [**time-range***time-range-name*]]

- For a numbered expert extended ACL, you can also run the following command in expert extended ACL mode to add an ACE:

  access-list *acl-id* { **permit** | **deny** } [*protocol*| [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[[VID** [*out*] **[inner** *in*]]] { *sourcesource-wildcard* | **host***source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host***destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence***precedence*] [**tos** *tos*] [**fragment**] [**range***lowerupper*] [**time-range***time-range-name*]]

Applying an Expert Extended ACL

By default, the expert extended ACL is not applied to any interface, that is, the created expert extended ACL does not filter incoming or outgoing L2 or L3 packets of a device.

Run the **expert access-group { *acl-id* | *acl-name* } { in| out }** command in interface/VXLAN configuration mode to apply an expert extended ACL to a specified interface/VXLAN.

14.3.4 IPv6 ACL

The IPv6 ACL implements refined control on incoming and outgoing IPv6 packets of a device. You can permit or deny the entry of specific IPv6 packets to a network according to actual requirements to control access of IPv6 users to network resources.

Working Principle

Define a series of IPv6 access rules in the IPv6 ACL, and then apply the ACL in the incoming or outgoing direction of an interface. The device checks whether the incoming or outgoing IPv6 packets match the rules and accordingly forwards or blocks these packets.

To configure an IPv6 ACL, you must specify a unique name for this ACL.

- Unlike the IP ACL, MAC extended ACL, and expert extended ACL, you can specify only a name but not an ID for the IPv6 ACL created.
- Only one IP ACL, or one MAC extended ACL, or one expert extended ACL can be applied to the incoming or outgoing direction of an interface. Besides, one more IPv6 ACL can be applied.

Implicit "Deny All Traffic" Rule Statement

At the end of every IPv6 ACL is an implicit "deny all IPv6 traffic" rule statement. Therefore, if a packet does not match any rule, the packet will be denied.

For example:

```
ipv6 access-list ipv6_acl
 10 permit ipv6 host 200::1 any
```

This ACL permits only IPv6 packets from the source host 200::1, and denies IPv6 packets from all other hosts. This is because the following statement exists at the end of this ACL: deny ipv6 any any.

Although the IPv6 ACL contains the implicit "deny all IPv6 traffic" rule statement by default, it does not filter ND packets.

Input Sequence of Rule Statements

Every new rule is added to the end of an ACL and in front of the default rule statement. The input sequence of statements in an ACL is very important. It determines the priority of each statement in the ACL. When determining whether to forward or block packets, a device compares packets with rule statements based on the sequence that rule statements are created. After locating a matched rule statement, the device does not check any other rule statement.

If a rule statement is created and permits all IPv6 traffic, all subsequent statements will not be checked.

For example:

```
ipv6 access-list ipv6_acl
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

As the first rule statement permits all IPv6 packets, all IPv6 packets sent from the host 200::1 does not match the subsequent deny rule with the serial number of 20, and therefore will not be denied. After the device finds that packets match the first rule statement, it does not check the subsequent rule statements any more.

Related Configuration

Configuring an IPv6 ACL

By default, no IPv6 ACL is configured on a device.

Run the **ipv6 access-list *acl-name*** command in global configuration mode to create an IPv6 ACL and enter IPv6 ACL mode.

Adding ACEs to an IPv6 ACL

By default, a newly created IPv6 ACL contains an implicit ACE that denies all IPv6 packets. This ACE is hidden from users, but takes effect when the ACL is applied to an interface. That is, all IPv6 packets will be discarded. Therefore, if you want the device to receive or send some specific IPv6 packets, add some ACEs to the ACL.

Run the following command in IPv6 ACL mode to add an ACE:

[*sn*] {**permit** | **deny** } *protocol*{*src-ipv6-prefix/prefix-len* | **host***src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* |**any**} [**range***lower upper*] [**dscp***dscp*] [**flow-label** *flow-label*] [**fragment]** [**time-range***tm-rng-name*][**log**]

Applying an IPv6 ACL

By default, the IPv6 ACL is not applied to any interface, that is, the IPv6 ACL does not filter incoming or outgoing IPv6 packets of a device.

Run the **ipv6 traffic-filter *acl-name* { in| out }** command in interface/VXLAN configuration mode to apply an IPv6 ACL to a specified interface/VXLAN.

14.3.5 Security Channel

In some application scenarios, packets meeting some characteristics may need to bypass the checks of access control applications. For example, before DOT1X authentication, users are allowed to log in to a specified website to download the DOT1X authentication client. The security channel can be used for this purpose. When the security channel configuration command is executed to apply a secure ACL globally or to an interface or VXLAN, this ACL becomes a security channel.

Working Principle

The security channel is also an ACL, and can be configured globally or for a specified interface or VXLAN. When arriving at an interface, packets are check on the security channel. If meeting the matching conditions of the security channel, packets directly enters a switch without undergoing the access control, such as port security, Web authentication, 802.1x, and IP+MAC binding check. A globally applied security channel takes effect on all interfaces except exclusive interfaces.

- The deny ACEs in an ACL that is applied to a security channel do not take effect. In addition, this ACL does not contain an implicit "deny all traffic" rule statement at the end of the ACL. If packets do not meet matching conditions of the security channel, they are checked according to the access control rules in compliance with the relevant process.
- You can configure up to eight exclusive interfaces for the global security channel. In addition, you cannot configure interface-based security channel on these exclusive interfaces.
- If both port-based migratable authentication mode and security channel are applied to an interface, the security channel does not take effect.
- An IPv6 ACL cannot be configured as a security channel.
- Only switches support the security channel.

Related Configuration

Configuring an ACL

Before configuring the security channel, configure an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, or expert extended ACL.

Configuring a VXLAN Security Channel

By default, no VXLAN security channel is configured on a device.

Run the **security access-group** {*acl-id* | *acl-name*} command in VXLAN configuration mode to configure a VXLAN security channel.

Configuring a Global Security Channel

By default, no global security channel is configured on a device.

Run the **security global access-group** {*acl-id* | ***acl-name*** } command in global configuration mode to configure a global security channel.

Configuring an Exclusive Interface for the Global Security Channel

By default, no exclusive interface is configured for the global security channel on a device.

Run the **security uplink enable** command in interface configuration mode to configure a specified interface as the exclusive interface of the global security channel.

14.3.6 SVI Router ACL

By default, an ACL that is applied to an SVI also takes effect on L2 packets forwarded within a VLAN and L3 packets forwarded between VLANs. Consequently, users in the same VLAN may fail to communicate with each other. Therefore, a switchover method is provided so that the ACL that is applied to an SVI takes effect only on routing packets between VLANs.

Working Principle

By default, the SVI router ACL function is disabled, and an SVI ACL takes effect on L3 packets forwarded between VLANs and L2 packets forwarded within a VLAN. After the SVI router ACL function is enabled, the SVI ACL takes effect only on L3 packets forwarded between VLANs.

Related Configuration

Configuring an ACL

Before configuring the SVI router ACL, configure and apply an ACL. For details about how to configure an ACL, see the earlier descriptions about ACL configuration.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Applying an ACL

For details about how to apply an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL. Apply the ACL in SVI configuration mode.

Configuring the SVI Router ACL

Run the **svi router-acls enable** command in global configuration mode to enable the SVI router ACL so that the ACL that is applied to an SVI takes effect only on packets forwarded at L3, and not on packets forwarded at L2 within a VLAN.

14.4 Configuration

Configuration Item	Description and Command	
Configuring an IP ACL	(Optional) It is used to filter IPv4 packets.	
	ip access-list standard	Configures a standard IP ACL.
	ip access-list extended	Configures an extended IP ACL.
	permit host any time-range	Adds a permit ACE to a standard IP ACL.
	deny host any time-range	Adds a deny ACE to a standard IP ACL.
	permit host any host any tos dscp precedence fragment time-range	Adds a permit ACE to an extended IP ACL.
	deny host any host any tos dscp precedence fragment time-range	Adds a deny ACE to an extended IP ACL.
	ip access-group in out	Applies a standard or an extended IP ACL.
Configuring an MAC Extended ACL	(Optional) It is used to filter L2 packets.	
	mac access-list extended	Configures an MAC extended ACL.
	permit any host any host cos inner time-range	Adds a permit ACE to an MAC extended ACL.
	deny any host any host cos inner time-range	Adds a deny ACE to an MAC extended ACL.
	mac access-group in out	Applies an MAC extended ACL.
Configuring an Expert Extended ACL	(Optional) It is used to filter L2 and L3 packets.	
	expert access-list extended	Configures an expert extended ACL.
	permit cos inner VID inner host any host any host any host any precedence tos fragment range time-range	Adds a permit ACE to an expert extended ACL.
	deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range	Adds a deny ACE to an expert extended ACL.
	expert access-group in out	Applies an expert extended ACL.
Configuring an IPv6 Extended ACL	(Optional) It is used to filter IPv6 packets.	
	ipv6 access-list	Configures an IPv6 ACL.
	permit host any host any range dscp flow-label fragment time-range	Adds a permit ACE to an IPv6 ACL.

Configuration Item	Description and Command	
	deny host any host any range dscp flow-label fragment time-range	Adds a deny ACE to an IPv6 ACL.
	ipv6 traffic-filter in out	Applies an IPv6 ACL.
Configuring a Security Channel	⚠ (Optional) It is used to enable packets meeting some characteristics to bypass the checks of access control applications, such as the DOT1X and Web authentication.	
	security access-group	Enables the security channel in interface configuration mode.
	security global access-group	Enables the security channel in global configuration mode.
	security uplink enable	Configures an interface as the exclusive interface of the global security channel in interface configuration mode.
Configuring Comments for ACLs	⚠ (Optional) It is used to configure comments for an ACL or ACE so that users can easily identify the functions of the ACL or ACE.	
	list-remark	Configures a comment for an ACL in ACL configuration mode.
	access-list list-remark	Configures a comment for an ACL in global configuration mode.
	remark	Configures a comment for an ACE in ACL configuration mode.

14.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface/VXLAN to control all incoming and outgoing IPv4 packets of this interface/VXLAN. You can permit or deny the entry of specific IPv4 packets to a network to control access of IP users to network resources.

Notes

N/A

Configuration Steps

↘ Configuring an IP ACL

- (Mandatory) Configure an IP ACL if you want to control access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IP ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an IP ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv4 packets of the device are denied by default.

Applying an IP ACL

- (Mandatory) Apply an IP ACL to a specified interface/VXLAN if you want this ACL take effect.
- You can apply an IP ACL on a specified interface/VXLAN of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IP ACL:
- Run the **ping** command to verify that the IP ACL takes effect on the specified interface. For example, if an IP ACL is configured to prohibit a host with a specified IP address or hosts in a specified IP address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access related network resources to verify that the IP ACL takes effect on the specified interface. For example, access the Internet or access the FTP resources on the network through FTP.

Related Commands

Configuring an IP ACL

Command	**ip access-list** { **standard | extended** } {*acl-name* | *acl-id* }
Parameter Description	**standard**: Indicates that a standard IP ACL is created. **extended**: Indicates that an extended IP ACL is created. *acl-name*: Indicates the name of a standard or an extended IP ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID that uniquely identifies a standard or extended IP ACL. If this option is configured, a numbered ACL is created. If a standard IP ACL is created, the value range of *acl-id* is 1–99 and 1300–1999. If an extended IP ACL is created, the value range of *acl-id* is 100–199 and 2000–2699.
Command Mode	Configuration mode
Usage Guide	Run this command to configure a standard or an extended IP ACL and enter standard or extended IP ACL configuration mode. If you want to control access of users to network resources by checking the source IP address of each packet, configure a standard IP ACL. If you want to control access of users to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.

Adding ACEs to an IP ACL

- Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL:

Command	[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*]

Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 1300–1999. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in global configuration mode.It cannot be used to add ACEs to a named IP ACL.

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL:

Command	[*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** |

	destination destination-wildcard } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs in extended IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 2000–1999. *sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence

	number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the type of service (TOS) field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment: Indicates that only fragmented IP packets except the first fragments are filtered.** **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode.It cannot be used to add ACEs to a named extended IP ACL.

Applying an IP ACL

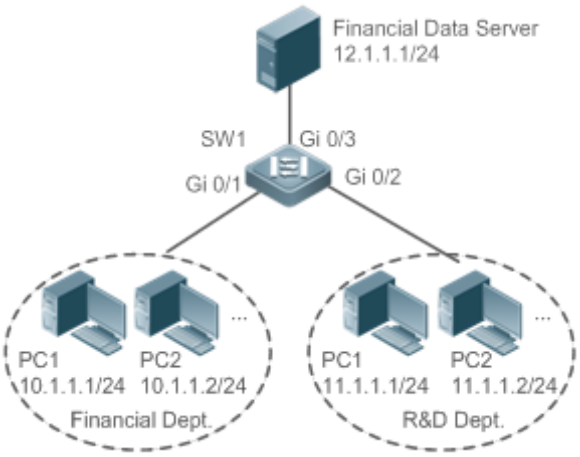
Command	**ip access-group** { *acl-id* **|** *acl-name* } { **in**	**out** } [**reflect**]
Parameter Description	*acl-id*: Indicates that a numbered standard or extended IP ACL will be applied to the interface. *acl-name*: Indicates that a named standard or extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming IP packets of the interface. **out**: Indicates that this ACL controls outgoing IP packets of the interface. **reflect:** Indicates that the reflexive ACL is enabled.
Command Mode	Interface configuration mode

Usage Guide	This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface/VXLAN.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server

Scenario **Figure 14-3**	
Configuration Steps	● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the outgoing direction of the interface connecting the financial data server.
SW1	sw1(config)#ip access-list standard 1 sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
Verification	● On a PC of the R&D department, ping the financial data server. Verify that the ping operation fails. ● On a PC of the financial department, ping the financial data server. Verify that the ping operation succeeds.
SW1	sw1(config)#show access-lists ip access-list standard 1

	10 permit 10.1.1.0 0.0.0.255 20 deny 11.1.1.0 0.0.0.255 sw1(config)#show access-group ip access-group 1 out Applied On interface GigabitEthernet 0/3

14.4.2 Configuring an MAC Extended ACL

Configuration Effect

Configure and apply an MAC extended ACL to an interface/VXLAN to control all incoming and outgoing IPv4 packets of this interface/VXLAN. You can permit or deny the entry of specific L2 packets to a network to control access of users to network resources based on L2 packets.

Notes

N/A

Configuration Steps

Configuring an MAC Extended ACL

- (Mandatory) Configure an MAC extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the MAC address of each user's PC.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The MAC extended ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an MAC Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming L2 Ethernet packets of the device are denied by default.

Applying an MAC extended ACL

- (Mandatory) Apply an MAC extended ACL to a specified interface if you want this ACL take effect.
- You can apply an MAC extended ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the MAC extended ACL:

- If an MAC extended ACL is configured to permit or deny some IP packets, run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, an MAC extended ACL is configured to prevent a device interface from receiving IP packets (Ethernet type is 0x0800), run the **ping** command for verification.
- If an MAC extended ACL is configured to permit or deny some non-IP packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- You can also construct L2 packets meeting some specified characteristics to check whether the MAC extended ACL takes effect. Typically, prepare two PCs, construct and send L2 packets on one PC, enable packet capturing on another PC, and check whether packets are forwarded as expected (forwarded or blocked) according to the action specified in the ACEs.

Related Commands

Configuring an MAC Extended ACL

Command	**mac access-list extended** {*acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an MAC extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID that uniquely identifies an MAC extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 700–799.
Command Mode	Configuration mode
Usage Guide	Run this command to configure an MAC extended ACL and enter MAC extended ACL configuration mode. You can configure an MAC extended ACL to control users' access to network resources by checking the L2 information of Ethernet packets.

Adding ACEs to an MAC Extended ACL

Use either of the following methods to add ACEs to an MAC extended ACL:

- Add ACEs in MAC extended ACL configuration mode.

Command	[*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr* } {**any** | **host** *dst-mac-addr* } [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE.

	any: Indicates that L2 packets sent from any host are filtered. **host** *src-mac-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **host** *dst-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that L2 packets with the specified class of service (cos) field in the outer tag are filtered. **inner** *cos*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	MAC extended ACL configuration mode
Usage Guide	Run this command to add ACEs in MAC extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an MAC extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr* } {**any** | **host** *dst-mac-addr* } [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 700–799. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *src-mac-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **host** *dst-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *cos*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **inner** *cos*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered MAC extended ACL in global configuration mode. It cannot be used to add ACEs to a named MAC extended ACL.

Applying an MAC Extended ACL

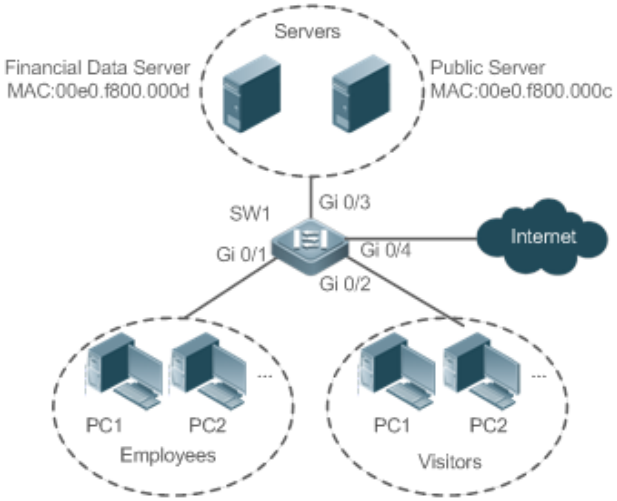
Command	**mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Parameter	*acl-id*: Indicates that a numbered MAC extended IP ACL will be applied to the interface.

Description	*acl-name*: Indicates that a named MAC extended IP ACL will be applied to the interface. **in**: Indicates that this ACL controls incoming L2 packets of the interface. **out**: Indicates that this ACL controls outgoing L2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an MAC extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an MAC Extended ACL to Restrict Resources Accessible by Visitors

Scenario **Figure 14-4**	
Configuration Steps	● Configure an MAC extended ACL. ● Add ACEs to the MAC extended ACL. ● Apply the MAC extended ACL to the outgoing direction of the interface connected to the visitor area so that visitors are allowed to access Internet and the public server of the company, but prohibited from accessing the financial data server of the company. That is, visitors cannot access the server with the MAC address 00e0.f800.000d.
SW1	sw1(config)#mac access-list extended 700 sw1(config-mac-nacl)#deny any host 00e0.f800.000d sw1(config-mac-nacl)#pemit any any sw1(config-mac-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in

Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
SW1	sw1(config)#show access-lists mac access-list extended 700 10 deny any host 00e0.f800.000d etype-any 20 permit any any etype-any sw1(config)#show access-group mac access-group 700 in Applied On interface GigabitEthernet 0/2

14.4.3 Configuring an Expert Extended ACL

Configuration Effect

Configure and apply an expert extended ACL to an interface/VXLAN to control incoming and outgoing packets of the interface/VXLAN based on the L2 and L3 information, and allow or prohibit the entry of specific packets to the network. In addition, you can configure an expert extended ACL to control all L2 packets based on the VLAN to permit or deny the access of users in some network segments to network resources. Generally, you can use an expert extended ACL if you want to incorporate ACEs of the IP ACL and MAC extended ACL into one ACL.

Configuration Steps

↘ Configuring an Expert Extended ACL

- (Mandatory) Configure an expert extended ACL if you want to control users' access to network resources based on the L2 packet header, for example, the VLAN ID.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The expert extended ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an Expert Extended ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming packets of the device are denied by default.

↘ Applying an Expert Extended ACL

- (Mandatory) Apply an expert extended ACL to a specified interface if you want this ACL take effect.
- You can apply an expert extended ACL in the incoming or outgoing direction of a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the expert extended ACL:
- If IP-based access rules are configured in an expert extended ACL to permit or deny some IP packets, run the **ping** command to verify whether these rules take effect.
- If MAC-based access rules are configured in an expert extended ACL to permit or deny some L2 packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- If VLAN ID-based access rules are configured in an expert extended ACL to permit or deny some L2 packets in some network segments (e.g., to prevent communication between VLAN 1 users and VLAN 2 users), ping PCs of VLAN 2 on a PC of VLAN 1. If the ping operation fails, the rules take effect.

Related Commands

Configuring an Expert Extended ACL

Command	**expert access-list extended** {*acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an expert extended ACL. If this option is configured, a named ACL is created. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out". *acl-id*: Indicates the ID of an expert extended ACL. If this option is configured, a numbered ACL is created. The value range of *acl-id* is 2700-2899.
Command Mode	Configuration mode
Usage Guide	Run this command to configure an expert extended ACL and enter expert extended ACL configuration mode.

Adding ACEs to an Expert Extended ACL

Use either of the following methods to add ACEs to an expert extended ACL:

- Add ACEs in expert extended ACL configuration mode.

Command	[*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] **[** [**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command.

	permit: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *out*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered. **VID inner** *in*: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the TOS field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Expert extended ACL configuration mode
Usage Guide	Run this command to add ACEs in expert extended ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an expert extended ACL in global configuration mode.

Command	**access-list** *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence**

	precedence] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]
Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 2700-2899. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IP protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. *ethernet-type*: Indicates that L2 packets of the specified Ethernet type are filtered. **cos** *out*: Indicates that L2 packets with the specified cos field in the outer tag are filtered. **cos inner** *in*: Indicates that L2 packets with the specified cos field in the inner tag are filtered. **VID** *out*: Indicates that L2 packets with the specified VLAN ID field in the outer tag are filtered. **VID inner** *in*: Indicates that L2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that L2 packets sent to any host are filtered. **precedence** *precedence:* Indicates that IP packets with the specified precedence field in the header are filtered. **tos** *tos:* Indicates that IP packets with the specified the TOS field in the header are filtered. **dscp** *dscp*: Indicates that IP packets with the specified the dcsp field in the header are filtered. **fragment:** Indicates that only fragmented IP packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	Expert extended ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered expert extended ACL in global configuration mode. It cannot be used to add ACEs to a named expert extended ACL.

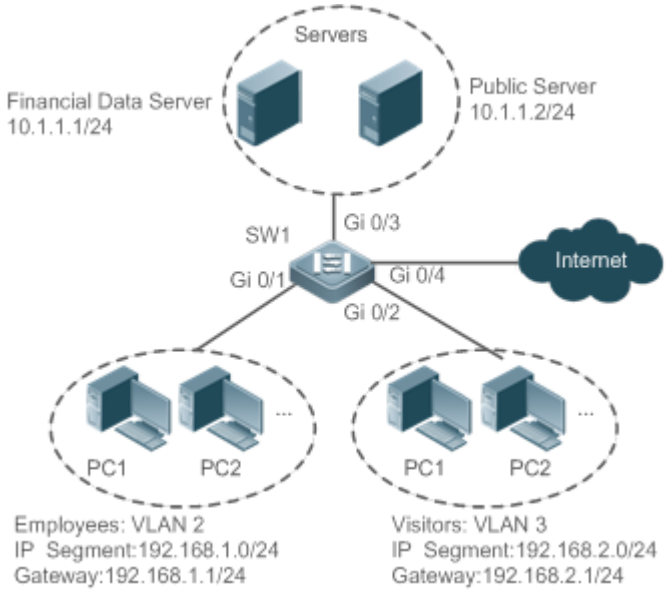
↘ Applying an Expert Extended ACL

Command	**expert access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }
Parameter Description	● *acl-id*: Indicates that a numbered expert extended ACL will be applied to the interface. ● *acl-name*: Indicates that a named expert extended ACL will be applied to the interface. ● **in**: Indicates that this ACL controls incoming L2 packets of the interface. ● **out**: Indicates that this ACL controls outgoing L2 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an expert extended ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an Expert Extended ACL to Restrict Resources Accessible by Visitors (It is required that visitors and employees cannot communicate with each other, visitors can access the public resource server but not the financial data server of the company.)

Scenario Figure 14-5	
Configuration Steps	● Configure an expert extended ACL. ● Add an ACE to deny packets sent from PCs in the visitor area (VLAN 3) to employee PCs in VLAN 2. ● Add an ACE to prevent visitors from accessing the financial data server of the company. ● Add an ACE to permit all packets. ● Apply the ACL to the incoming direction of the interface of the switch that connects to the visitor area.
SW1	sw1(config)#expert access-list extended 2700 sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any

	sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any sw1(config-exp-nacl)#pemit any any any any sw1(config-exp-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
Verification	● On a visitor's PC, ping the financial data server. Verify that the ping operation fails. ● On a visitor's PC, ping the public resource server. Verify that the ping operation succeeds. ● On a visitor's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails. ● On a visitor's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.
SW1	sw1(config)#show access-lists expert access-list extended 2700 10 deny ip any any 192.168.1.0 0.0.0.255 any 20 deny ip any any host 10.1.1.1 any 30 permit ip any any any any sw1(config)#show access-group expert access-group 2700 in Applied On interface GigabitEthernet 0/2

14.4.4 Configuring an IPv6 Extended ACL

Configuration Effect

Configure and apply an IPv6 ACL to an interface/VXLAN to control all incoming and outgoing IPv5 packets of this interface/VXLAN. You can permit or deny the entry of specific IPv6 packets to a network to control access of IPv6 users to network resources.

Configuration Steps

↘ Configuring an IPv6 ACL

- (Mandatory) Configure an IP ACL if you want to access of IPv4 users to network resources.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an IPv6 ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, all incoming IPv6 packets of the device are denied by default.

Applying an IPv6 ACL

- (Mandatory) Apply an IPv6 ACL to a specified interface on a device if you want this ACL take effect.
- You can apply an IPv6 ACL on a specified interface/VXLAN of an access, an aggregate, or a core device based on the distribution of users.

Verification

- Use the following methods to verify the configuration effects of the IPv6 ACL:
- Run the **ping** command to verify that the IPv6 ACL takes effect on the specified interface. For example, if an IPv6 ACL is configured to prohibit a host with a specified IP address or hosts in a specified IPv6 address range from accessing the network, run the **ping** command to verify that the host(s) cannot be successfully pinged.
- Access network resources, for example, visit an IPv6 website, to check whether the IPv6 ACL takes effect on the specified interface.

Related Commands

Configuring an IPv6 ACL

Command	**ipv6 access-list** *acl-name*
Parameter Description	*acl-name*: Indicates the name of a standard or an extended IP ACL. The name is a string of 1 to 99 characters. The ACL name cannot start with numbers (0–9), "in", or "out".
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an IPv6 ACL and enter IPv6 configuration mode.

Adding ACEs to an IPv6 ACL

- To filter TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*] {**permit** | **deny** } *protocol* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any**} [*op dstport* | **range** *lower upper*] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment]** [**time-range***tm-rng-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE.

	protocol: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol numbers, including icmp, ipv6, tcp, and udp. *src-ipv6-prefix/prefix-len:* Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered. **host** *src-ipv6-addr*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *dst-ipv6-pfix/pfix-len:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered. **host** *dst-ipv6-addr*: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. *op dstport*: Indicates that TCP or UDP packets are filtered based on the L4 destination port number. The value of the **op** parameter can be **eq** (equal to), **neq** (not equal to), **gt** (greater than), or **lt** (smaller than). **range** *lower upper*: Indicates that TCP or UDP packets with the L4 destination port number in the specified range are filtered. **dscp** *dscp*: Indicates that IPv6 packets with the specified the dcsp field in the header are filtered. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **fragment:** Indicates that only fragmented IPv6 packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

- To filter IPv6 packets except for the TCP or UDP packets, add ACEs to an IPv6 ACL as follows:

Command	[*sn*] { **permit** | **deny** } *protocol* { *src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any** } { *dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any** } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range***tm-rng-name*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value ranges from 1 to 2,147,483,647. This sequence number determines the priority of this ACE in the ACL. A smaller sequence number indicates a higher priority. An ACE with a higher priority will be preferentially used to match packets. If you do not specify the sequence number when adding an ACE, the system automatically allocates a sequence number, which is equal to an increment (10 by default) plus the sequence number of the last ACE in the current ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a newly-added ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate the use, the system provides frequently-used abbreviations of IPv6 protocol numbers to replace the specific IP protocol

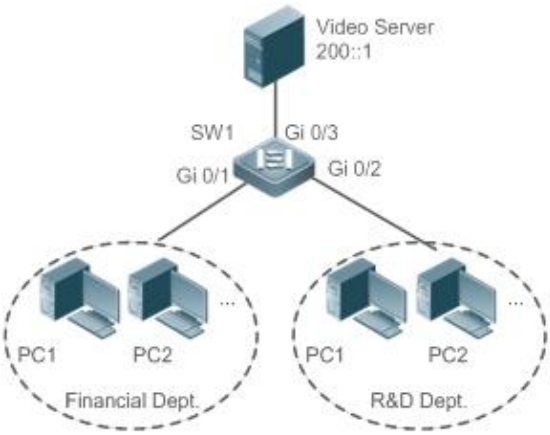
	numbers, including icmp, ipv6, tcp, and udp. *src-ipv6-prefix/prefix-len:* Indicates that IP packets sent from hosts in the specified IPv6 network segment are filtered. **host** *src-ipv6-addr*: Indicates that IPv6 packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IPv6 packets sent from any host are filtered. *dst-ipv6-pfix/pfix-len:* Indicates that IPv6 packets sent from hosts in the specified IPv6 network segment are filtered. **host** *dst-ipv6-addr*: Indicates that IPv6 packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IPv6 packets sent to any host are filtered. **dscp** *dscp*: Indicates that IPv6 packets with the specified the dcsp field in the header are filtered. **flow-label** *flow-label*: Indicates that IPv6 packets with the specified the flow label field in the header are filtered. **fragment:** Indicates that only fragmented IPv6 packets except the first fragments are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. For details about the time range, see the configuration manual of the time range.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

Applying an IPv6 ACL

Command	**ipv6 traffic-filter** *acl-name* { **in** | **out** }
Parameter Description	*acl-name*: Indicates the name of an IPv6 ACL. **in**: Indicates that this ACL controls incoming IPv6 packets of the interface. **out**: Indicates that this ACL controls outgoing IPv6 packets of the interface.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IPv6 ACL take effect on the incoming or outgoing packets of the specified interface.

Configuration Example

Configuring an IPv6 ACL to Prohibit the R&D Department from Accessing the Video Server

Scenario **Figure 14-6**	
Configuration Steps	● Configure an IPv6 ACL. ● Add an ACE to the IPv6 ACL to prevent access to the video server. ● Add an ACE to the IPv6 ACL to permit all IPv6 packets. ● Apply the IPv6 ACL to the incoming direction of the interface connected to the R&D department.
SW1	sw1(config)#ipv6 access-list dev_deny_ipv6video sw1(config-ipv6-nacl)#deny ipv6 any host 200::1 sw1(config-ipv6-nacl)#permit ipv6 any any sw1(config-ipv6-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
Verification	● On a PC of the R&D department, ping the video server. Verify that the ping operation fails.
SW1	sw1(config)#show access-lists ipv6 access-list dev_deny_ipv6video 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Applied On interface GigabitEthernet 0/2

14.4.5 Configuring a Security Channel

Configuration Effect

Configure a security channel to enable packets meeting the security channel rules to bypass the checks of access control applications. Configure the security channel if an access control application (such as DOT1X) is enabled on an uplink interface of a user, but the user should be allowed to log in to a website to download some resources (for example, downloading the Ruijie SU client) before the DOT1X authentication.

Configuration Steps

↘ Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

↘ Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured for an ACL, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

↘ Configuring a Security Channel on a Specified Interface, VXLAN or Globally

- Configure a security channel on an interface if you want this security channel to take effect on the interface. Configure a VXLAN security channel if you want this security channel to take effect on VNI. Configure a global security channel if you want this security channel to take effect globally. You must configure either the interface-based security channel or the global security channel.
- You can configure a security channel on an access, an aggregate, or a core device based on the distribution of users.

↘ Configuring an Exclusive Interface for the Global Security Channel

- (Optional) Configure an interface as the exclusive interface for the global security channel if you do not want the global security channel to take effect on this interface.

↘ Configuring an Access Control Application

- (Optional) You can enable the DOT1X or Web authentication function to verify the security channel function.
- You can configure the access control function on an access, an aggregate, or a core device based on the distribution of users.

Verification

On a PC that is subject to the control of an access control application, ping the resources (devices or servers) that are allowed to bypass the check of the access control application to verify the configuration of the security channel.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Security Channel on an Interface

Command	**security access-group** {*acl-id* | *acl-name* }
Parameter Description	*acl-id*: Indicates that ID of the ACL that is configured as the security channel. *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure a specified ACL as the security channel on the specified interface.

Configuring a Global Security Channel

Command	**security global access-group** {*acl-id* | *acl-name* }
Parameter Description	*acl-id*: Indicates that ID of the ACL that is configured as the security channel. *acl-name*: Indicates that name of the ACL that is configured as the security channel.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the specified ACL as the global security channel.

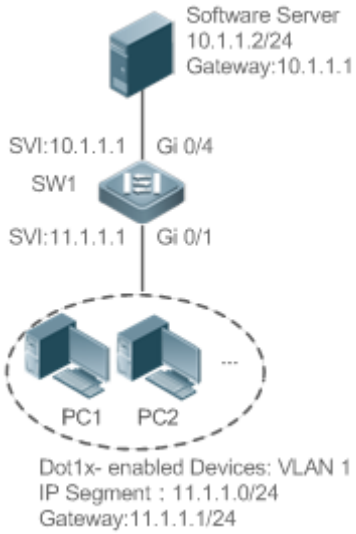
Configuring an Exclusive Interface for the Global Security Channel

Command	**security uplink enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the specified interface as the exclusive interface of the global security channel.

Configuration Example

The following configuration example describes only ACL-related configurations.

Enabling DOT1X Authentication and Configuring a Security Channel to Allow Users to Download the SU Software From the Server Before Authentication

Scenario **Figure 14-7**	
Configuration Steps	● Configure an expert extended ACL "exp_ext_esc". ● Add an ACE to allow forwarding packets to the destination host 10.1.1.2. ● Add an ACE to permit the DHCP packets. ● Add an ACE to permit the ARP packets. ● On the interface where DOT1X authentication is enabled, configure the ACL "exp_ext_esc" as the security channel.
SW1	sw1(config)#expert access-list extended exp_ext_esc sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any sw1(config-exp-nacl)# permit 0x0806 any any any any any sw1(config-exp-nacl)# permit tcp any any any any eq 67 sw1(config-exp-nacl)# permit tcp any any any any eq 68 sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
Verification	● On a PC of the sales department, ping the server of the sales department. Verify that the ping operation succeeds. ● On the PCs of R&D department 1 and R&D department 2, ping the server of the sales department. Verify that the ping operations fail.
	sw1#show access-lists expert access-list extended exp_ext_esc 10 permit ip any any host 10.1.1.2 any 20 permit arp any any any any any 30 permit tcp any any any any eq 67

	40 permit tcp any any any any eq 68…… sw1#show running-config interface gigabitEthernet 0/1 Building configuration... Current configuration : 59 bytes interface GigabitEthernet 0/1 security access-group exp_ext_esc

14.4.6 Configuring the Time Range-Based ACEs

Configuration Effect

Configure the time range-based ACEs if you want some ACEs to take effect or to become invalid in a specified period of time, for example, in some time ranges during a week.

Configuration Steps

↘ Configuring an ACL

- (Mandatory) Configure an ACL if you want ACEs to take effect in the specified time range. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

↘ Adding an ACE with the Time Range Specified

- (Mandatory) Specify the time range when adding an ACE. For details about how to configure the time range, see the configuration manual related to the time range.

↘ Applying an ACL

- (Mandatory) Apply the ACL to a specified interface if you want to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access, an aggregate, or a core device based on the distribution of users.

Verification

In the time range that the configured ACE takes effect or becomes invalid, run the **ping** command or construct packets matching the ACE to check whether the ACE takes effect or becomes invalid.

Related Commands

Configuring an ACL

For details about the ACL configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Adding an ACE with the Time Range Specified

For details about the ACE configuration commands, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

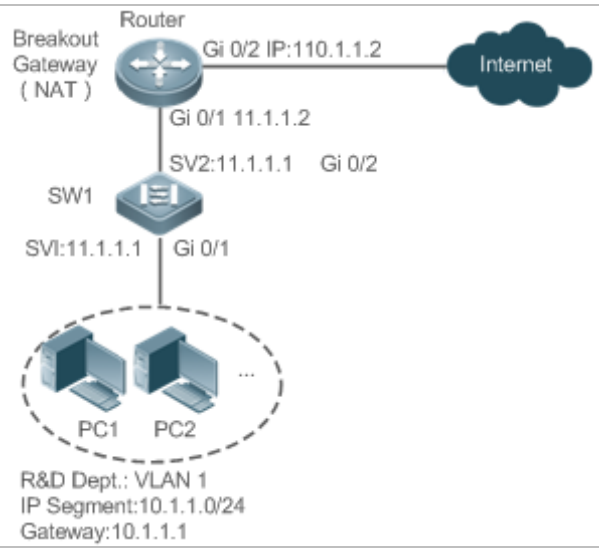
Applying an ACL

For details about the command for applying an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuration Example

The following configuration example describes only ACL-related configurations.

Adding an ACE With the Time Range Specified to Allow the R&D Department to Access the Internet Between 12:00 and 13:30 Every Day

Scenario **Figure 14-8**	
Configuration Steps	● Configure a time range named "access-internet", and add an entry of the time range between 12:00 and 13:30 every day. ● Configure an IP ACL "ip_std_internet_acl". ● Add an ACE to allow packets with the source IP address in the network segment 10.1.1.0/24, and associate this ACE with the time zone "access-internet". ● Add an ACE to deny packets with the source IP address the network segment 10.1.1.0/24. Access to the Internet is not allowed except in the specified time range. ● Add an ACE to permit all packets. ● Apply the ACL to the outgoing direction of the interface connected to the breakout gateway.

SW1	Ruijie(config)# time-range access-internet Ruijie(config-time-range)# periodic daily 12:00 to 13:30 Ruijie(config-time-range)# exit sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
Verification	● Within the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website can be opened normally. ● Beyond the time range between 12:00 and 13:30, visit the Baidu website on a PC of the R&D department. Verify that the website cannot be opened.
SW1	sw1#show time-range time-range entry: access-internet (inactive) periodic Daily 12:00 to 13:30 sw1#show access-lists ip access-list standard ip_std_internet_acl 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive) 20 deny 10.1.1.0 0.0.0.255 30 permit any sw1#show access-group ip access-group ip_std_internet_acl out Applied On interface GigabitEthernet 0/2

14.4.7 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if a lot of ACLs are configured without any comments, it is difficult to distinguish these ACLs later on. You can configure comments for ACLs to better understand the intended use of ACLs.

Configuration Steps

Configuring an ACL

- (Mandatory) Configure an ACL before configuring the security channel. For details about the configuration method, see the earlier descriptions.
- You can configure this ACL on an access, an aggregate, or a core device based on the distribution of users. The configurations take effect only on the local device, and do not affect other devices on the network.

Configuring Comments for ACLs

- (Optional) Configure comments for ACLs so that it is easy to manage and understand the configured ACLs.

Adding ACEs to an ACL

- (Optional) An ACL may contain zero or multiple ACEs. If no ACE is configured, it is equivalent that the security channel does not take effect. For details about how to add an ACE to an ACL, see the related descriptions.

Configuring Comments for ACEs

- (Optional) To facilitate understanding of a configured ACL, you can configure comments for ACEs in addition to comments for the ACL.

Verification

Run the **show access-lists** command on the device to display the comments configured for ACLs.

Related Commands

Configuring an ACL

For details about how to configure an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring a Comment for an ACL

Use either of the following two methods to configure a comment for an ACL:

Command	**list-remark** *comment*
Parameter Description	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command	ACL configuration mode

Mode	
Usage Guide	Run this command to configure the comment for a specified ACL.

Command	**access-list** *acl-id* **list-remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see the earlier descriptions about the IP ACL, MAC extended ACL, expert extended ACL, or IPv6 ACL.

Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE:

Command	**remark** *comment*
Parameter Description	***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

Command	**access-list** *acl-id* **remark** *comment*
Parameter Description	***acl-id***: Indicates the ID of an ACL. ***comment***: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE.

14.5 Monitoring

Clearing

Description	Command
Clears the ACL packet matching counters.	**clear counters access-list** [*acl-id* | *acl-name*]

Displaying

Description	Command
Displays the basic ACLs.	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
Displays the redirection ACEs bound to a specified interface. If the interface is not specified, redirection ACEs bound to all interfaces are displayed.	**show redirect** [**interface** *interface-name*]
Displays the ACL configurations applied to an interface.	**show access-group** [**interface** *interface-name*]
Displays the IP ACL configurations applied to an interface.	**show ip access-group** [**interface** *interface-name*]
Displays the MAC extended ACL configurations applied to an interface.	**show mac access-group** [**interface** *interface-name*]
Displays the expert extended ACL configurations applied to an interface.	**show expert access-group** [**interface** *interface-name*]
Displays the IPv6 ACL configurations applied to an interface.	**show ipv6 traffic-filter** [**interface** *interface-name*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the ACL running process.	**debug acl acld event**
Debugs the ACL clients.	**debug acl acld client-show**
Debugs the ACLs created by all ACL clients.	**debug acl acld acl-show**

15 Configuring TACACS+

15.1 Overview

TACACS+ is a security protocol enhanced in functions based on the Terminal Access Controller Access Control System (TACACS) protocol. It is used to implement the authentication, authorization, and accounting (AAA) of multiple users.

Protocols and Standards

- RFC 1492 Terminal Access Controller Access Control System

15.2 Applications

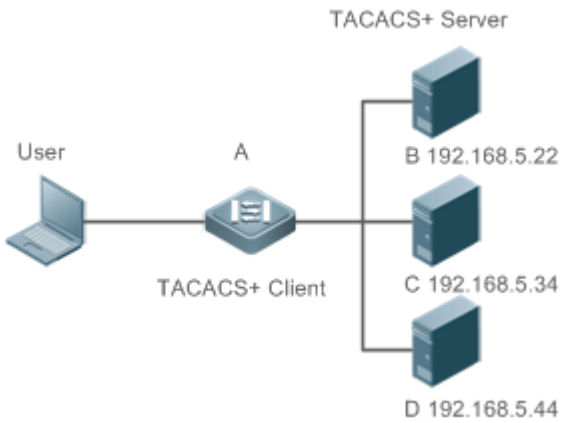
Application	Description
Managing and Controlling Login of End Users	Password verification and authorization need to be conducted on end users.

15.2.1 Managing and Controlling Login of End Users

Scenario

TACACS+ is typically applied in the login management and control of end users. A network device serves as the TACACS+ client and sends a user name and password to the TACACS+ server for verification. The user is allowed to log in to the network device and perform operations after passing the verification and obtaining authorization. See the following figure.

Figure 15-1



Remarks	● A is a client that initiates TACACS+ requests. ● B, C, and D are servers that process TACACS+ requests.

Deployment

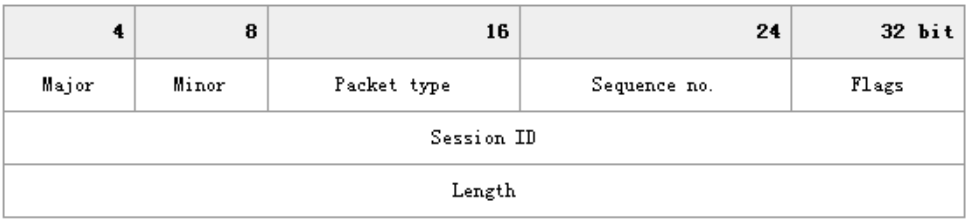
- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the access device (Device A) so that the servers provide TACACS+-based AAA function for the access device. Enable the AAA function on Device A to start authentication for the user login.
- Enable the TACACS+ client function on Device A, add the IP addresses of the TACACS+ servers (Server B, Server C, and Server D) and the shared key so that Device A communicates with the TACACS+ servers over TACACS+ to implement the AAA function.

15.3 Features

Basic Concepts

↘ Format of TACACS+ Packets

Figure 15-2



- Major Version: Indicates the major TACACS+ version number.
- Minor Version: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets, with the options including:
  TAC_PLUS_AUTHEN: = 0x01 (authentication);
  TAC_PLUS_AUTHOR: = 0x02 (authorization);
  TAC_PLUS_ACCT: = 0x03 (accounting)
- Sequence Number: Indicates the sequence number of a data packet in the current session. The sequence number of the first TACACS+ data packet in a session must be 1 and the sequence number of subsequent each data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. One of the bits in the value specifies whether data packets need to be encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

Overview

Feature	Description

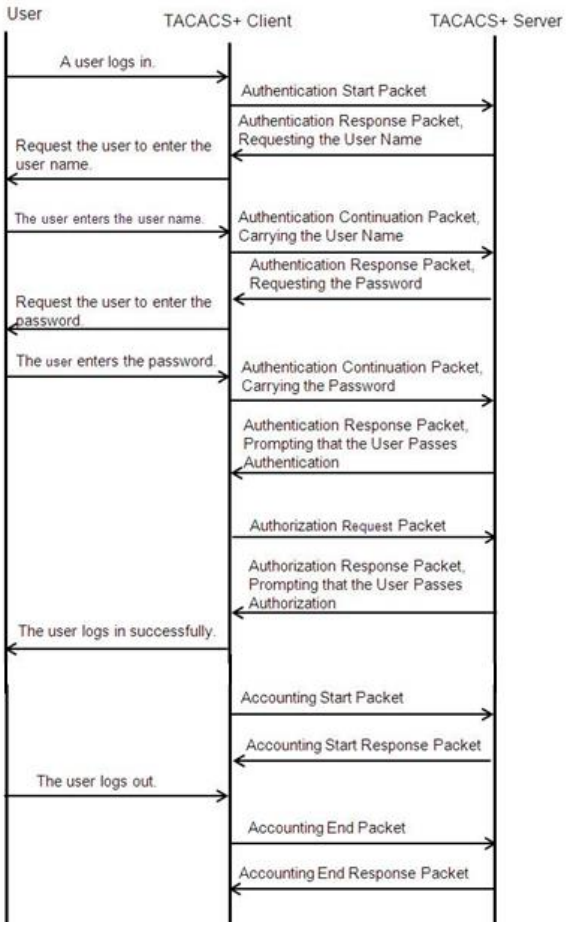
TACACS+ Authentication, Authorization, and Accounting	Conducts authentication, authorization, and accounting on end users.

15.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

The following figure uses basic authentication, authorization, and accounting of user login to describe interaction of TACACS+ data packets.

Figure 15-3



The entire basic message interaction process includes three sections:

1. The authentication process is described as follows:
    1) A user requests to log in to a network device.
    2) After receiving the request, the TACACS+ client sends an authentication start packet to the TACACS+ server.
    3) The TACACS+ server returns an authentication response packet, requesting the user name.
    4) The TACACS+ client requests the user to enter the user name.

5) The user enters the login user name.

6) After receiving the user name, the TACACS+ client sends an authentication continuation packet that carries the user name to the TACACS+ server.

7) The TACACS+ server returns an authentication response packet, requesting the login password.

8) The TACACS+ client requests the user to enter the login password.

9) The user enters the login password.

10) After receiving the login password, the TACACS+ client sends an authentication continuation packet that carries the login password to the TACACS+ server.

11) The TACACS+ server returns an authentication response packet, prompting that the user passes authentication.

2. The user authorization starts after successful authentication:

1) The TACACS+ client sends an authorization request packet to the TACACS+ server.

2) The TACACS+ server returns an authorization response packet, prompting that the user passes authorization.

3) After receiving the authorization success packet, the TACACS+ client outputs the network device configuration screen for the user.

3. Accounting and audit need to be conducted on the login user after successful authorization:

1) The TACACS+ client sends an accounting start packet to the TACACS+ server.

2) The TACACS+ server returns an accounting response packet, prompting that the accounting start packet has been received.

3) The user logs out.

4) The TACACS+ client sends an accounting end packet to the TACACS+ server.

5) The TACACS+ server returns an accounting response packet, prompting that the accounting end packet has been received.

15.4 Configuration

Configuration	Description and Command	
Configuring TACACS+ Basic Functions	⚠ (Mandatory) It is used to enable the TACACS+ security service.	
	tacacs-server host	Configures the TACACS+ server.
	tacacs-server key	Specifies the key shared by the server and network device.
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server.

Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	⚠ (Optional) It is used to separately process authentication, authorization, and accounting requests.	
	aaa group server tacacs+	Configures TACACS+ server groups and divides TACACS+ servers into different groups.
	server	Adds servers to TACACS+ server groups.

15.4.1 Configuring TACACS+ Basic Functions

Configuration Effect

- The TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the method of using TACACS+ to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates the authentication, authorization, and accounting requests to configured TACACS+ servers according to the configured sequence. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Enabling AAA

- Mandatory. The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	The AAA function is disabled.
Command Mode	Global configuration mode
Usage Guide	The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

↘ Configuring the IP Address of the TACACS+ Server

- Mandatory. Otherwise, a device cannot communicate with the TACACS+ server to implement the AAA function.

Command	**tacacs-server host** {*ipv4-address* | *ipv6-address*} [**port***integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server. **port***integer*: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49. **timeout** *integer*: Indicates the timeout time of the communication with the TACACS+ server. The global timeout time is used by default. **key** [**0** | **7**] *text-string*: Indicates the shared key of the server. The global key is used if it is not configured. An encryption type can be specified for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.
Defaults	No TACACS+ server is configured.
Command Mode	Global configuration mode
Usage Guide	1. You can specify the shared key of the server when configuring the IP address of the server. If no shared key is specified, the global key configured using the **tacacs-server key** command is used as the shared key of the server. The shared key must be completely the same as that configured on the server. 2. You can specify the communication port of the server when configuring the IP address. 3. You can specify the communication timeout time of the server when configuring the IP address.

Configuring the Shared Key of the TACACS+ Server

- Optional.
- If no global communication protocol is configured using this command, set **key** to specify the shared key of the server when running the **tacacs-server host** command to add server information. Otherwise, a device cannot communicate with the TACACS+ server.
- If no shared key is specified by using **key** when you run the **tacacs-server host** command to add server information, the global key is used.

Command	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption.
Defaults	No shared key is configured for any TACACS+ server.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure a global shared key for servers. To specify a different key for each server, set **key** when running the **tacacs-server host** command.

Configuring the Timeout Time of the TACACS+ Server

- Optional.
- You can set the timeout time to a large value when the link between the device and the server is unstable.

Command	**tacacs-server timeout***seconds*
Parameter Description	*seconds*: Indicates the timeout time, with the unit of seconds. The value ranges from 1 second to 1,000 seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the global server response timeout time. To set different timeout time for each server, set **timeout** when running the **tacacs-server host** command.

Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable the device to interact with the TACACS+ server and conduct packet capture to check the TACACS+ interaction process between the device and the TACACS+ server.
- View server logs to check whether the authentication, authorization, and accounting are normal.

Configuration Example

Using TACACS+ for Login Authentication

Scenario **Figure 15-4**	
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure the method of using TACACS+ for authentication. ● Apply the configured authentication method on an interface.
A	Ruijie# configure terminal Ruijie(config)# aaa new-model Ruijie(config)# tacacs-server host 192.168.5.22 Ruijie(config)# tacacs-server key aaa

	Ruijie(config)# aaa authentication login test group tacacs+ Ruijie(config)# line vty 0 4 Ruijie(config-line)# login authentication test
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. View the authentication log of the user on the TACACS+ server.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- No method list is configured.

15.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

Configuration Effect

- The authentication, authorization, and accounting in the security service are processed by different TACACS+ servers, which improves security and achieves load balancing to a certain extent.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Configuring TACACS+ Server Groups

- Mandatory. There is only one TACACS+ server group by default, which cannot implement separate processing of authentication, authorization, and accounting.
- Three TACACS+ server groups need to be configured for separately processing authentication, authorization, and accounting.

Command	**aaa group server tacacs+***group-name*
Parameter Description	*group-name*: Indicates the name of a group. A group name cannot be radius or tacacs+, which are the names of embedded groups.
Defaults	No TACACS+ server group is configured.
Command Mode	Global configuration mode

Usage Guide	Group TACACS+ servers so that authentication, authorization, and accounting are completed by different server groups.

Adding Servers to TACACS+ Server Groups

- Mandatory. If no server is added to a server group, a device cannot communicate with TACACS+ servers.
- In server group configuration mode, add the servers that are configured using the **tacacs-server host** command.

Command	**server {***ipv4-address* | *ipv6-address*}
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For the address of a server configured in a TACACS+ server group, the server must be configured using the **tacacs-server host** command in global configuration mode. If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.

Configuring oob of a TACACS+ Server Group

- In server group configuration mode, specify routing for the communication of servers in the group.

Command	**ip oob**
Parameter Description	N/A
Defaults	No oob is specified by default.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. If no MGMT port is specified, the MGMT0 port is used by default.

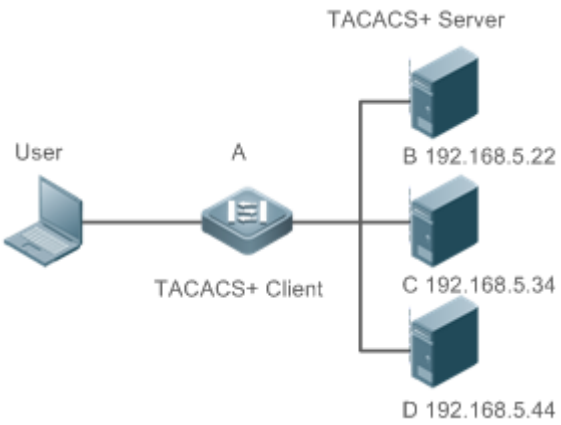
Verification

Configure the AAA method list that specifies to conduct authentication, authorization, and accounting on users by using TACACS+.

- Enable a device to interact with TACACS+ servers. Conduct packet capture, check that the authentication, authorization, and accounting packets are interacted with different servers, and check the source addresses in packets.

Configuration Example

Configuring Different TACACS+ Server Groups for Separately Processing Authentication, Authorization, and Accounting

Scenario **Figure 15-5**	
Remarks	● A is a client that initiates TACACS+ requests. ● B is a server that processes TACACS+ authentication requests. ● C is a server that processes TACACS+ authorization requests. ● D is a server that processes TACACS+ accounting requests.
Configuration Steps	● Enable AAA. ● Configure the TACACS+ server information. ● Configure TACACS+ server groups. ● Add servers to TACACS+ server groups. ● Configure the method of using TACACS+ for authentication. ● Configure the method of using TACACS+ for authorization. ● Configure the method of using TACACS+ for accounting. ● Apply the configured authentication method on an interface. ● Apply the configured authorization method on an interface. ● Apply the configured accounting method on an interface.
	Ruijie# configure terminal Ruijie(Ruijie(config)# aaa new-model Ruijie(config)# tacacs-server host 192.168.5.22 Ruijie(config)# tacacs-server host 192.168.5.34 Ruijie(config)# tacacs-server host 192.168.5.44 Ruijie(config)# tacacs-server key aaa Ruijie(config)# aaa group server tacacs+ tacgrp1 Ruijie(config-gs-tacacs)# server 192.168.5.22 Ruijie(config-gs-tacacs)# exit Ruijie(config)# aaa group server tacacs+ tacgrp2

	Ruijie(config-gs-tacacs)# server 192.168.5.34 Ruijie(config-gs-tacacs)# exit Ruijie(config)# aaa group server tacacs+ tacgrp3 Ruijie(config-gs-tacacs)# server 192.168.5.44 Ruijie(config-gs-tacacs)# exit Ruijie(config)# aaa authentication login test1 group tacacs+ Ruijie(config)# aaa authentication enable default group tacgrp1 Ruijie(config)# aaa authorization exec test2 group tacgrp2 Ruijie(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 Ruijie(config)# line vty 0 4 Ruijie(config-line)# login authentication test1 Ruijie(config-line)#authorization exec test2 Ruijie(config-line)# accounting commands 15 test3
Verification	Telnet to a device from a PC. The screen requesting the user name and password is displayed. Enter the correct user name and password to log in to the device. Enter the **enable** command and enter the correct **enable** password to initiate **enable** authentication. Enter the privilege EXEC mode after passing the authentication. Perform operations on the device and then exit the device. View the authentication log of the user on the server with the IP address of 192.168.5.22. View the **enable** authentication log of the user on the server with the IP address of 192.168.5.22. View the **exec** authorization log of the user on the server with the IP address of 192.168.5.34. View the command accounting log of the user on the server with the IP address of 192.168.5.44.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.
- No method list is configured.

15.5 Monitoring

Displaying

Description	Command
Displays interaction with each TACACS+ server.	**show tacacs**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs TACACS+.	**debug tacacs+**

16 Configuring SCC

16.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access control and network security services, so that these access control and network security services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services are dot1x, Web authentication, Address Resolution Protocol (ARP) check, and IP Source Guard. The network security services include Access Control List (ACL), Network Foundation Protection Policy (NFPP), and anti-ARP gateway spoofing. When two or more access control or network security services are simultaneously enabled on the device, or when both access control and network security services are simultaneously enabled on the device, the SCC coordinates the coexistence of these services according to relevant policies.

For details about the access control and network security services, see the related configuration guide. This document describes the SCC only.

Protocol and Standards

N/A

16.2 Application

Typical Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet based on dot1x client authentication or Web authentication. ARP spoofing between the students should be prevented. In addition, terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

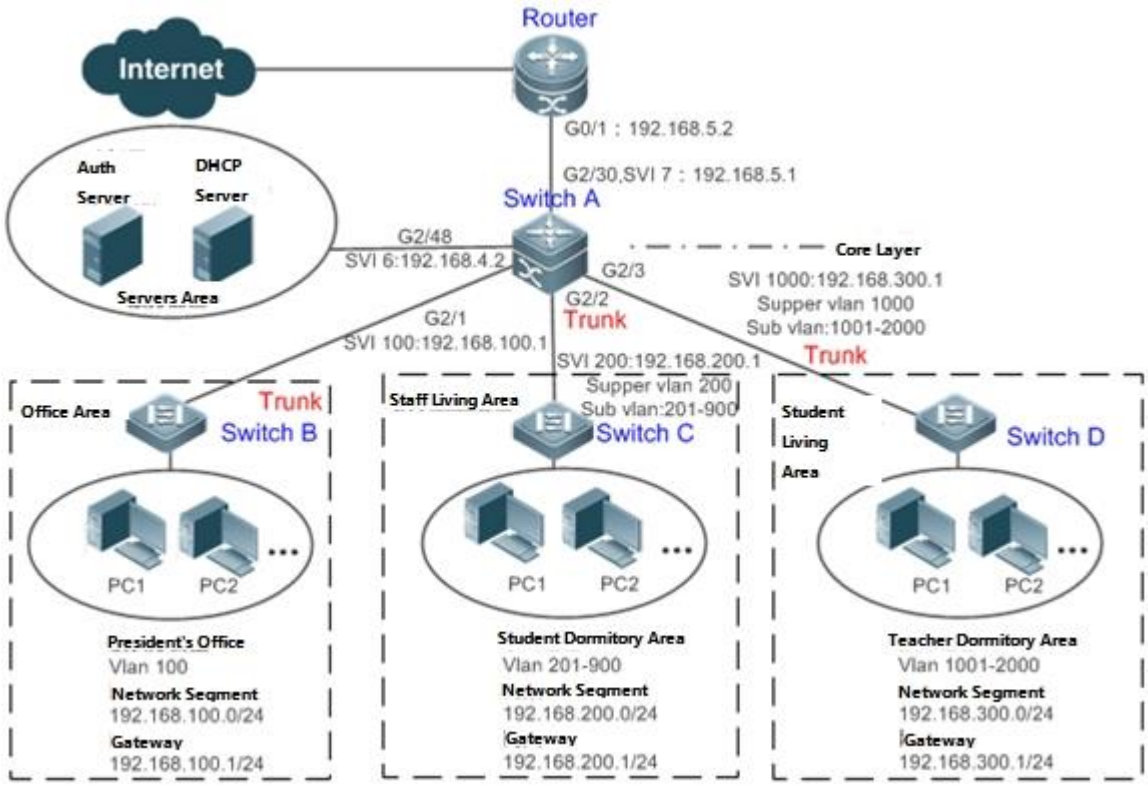
16.2.1 Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network of a university usually need to be authenticated through the dot1x client or Web before accessing the Internet, so as to facilitate accounting and guarantee the benefits of the university.

- The students can access the Internet through dot1x client authentication or Web authentication.
- ARP spoofing between the students is prevented, so as to guarantee the stability of the network.
- Terminal devices in some departments (such as the headmaster's office) can access the Internet without authentication.

Figure 16-1



Remarks	A traditional campus network is hierarchically designed, which consists of an access layer, a convergence layer and a core layer, where the access layer performs user access control. On an extended Layer 2 campus network, however, user access control is performed by a core switch, below which access switches exist without involving any convergence device in between. The ports between the core switch and the access switches (such as switches B, C, and D in Figure 16-1) are all trunk ports. The user access switches B, C, and D connect to PCs in various departments via access ports, and VLANs correspond to sub VLANs configured on the downlink ports of the core switch, so that access users are in different VLANs to prevent ARP spoofing. The core switch A connects to various servers, such as the authentication server and the DHCP server. Super VLANs and sub VLANs are configured on the downlink ports. One super VLAN correspond to multiple sub VLANs, and each sub VLAN represents an access user.

Deployment

- On the core switch, different access users are identified by VLAN and port numbers. Each access user (or a group of access users) corresponds to one VLAN. The ports on each access switch that connect to downstream users are configured as access ports, and one user VLAN is assigned to each access user according to VLAN planning. The core switch does not forward ARP requests. The core switch replies to the ARP requests from authenticated users only, so as to prevent ARP spoofing. On the core switch A, user VLANs are regarded as sub VLANs, super VLANs are configured, and SVIs corresponding to the super VLANs are configured as user gateways.

- On the downlink ports of the core switch (switch A in this example) that connect to the teachers' living area and the students' living area, both dot1x authentication and Web authentication are enabled, so that users can freely select either authentication mode for Internet access.
- Any special department (such as the headmaster's office in this example) can be allocated to a particular VLAN, and this VLAN can be configured as an authentication-exemption VLAN so that users in this department can access the Internet without authentication.

16.3 Basic Concepts

User Online-Status Detection

For a chargeable user, accounting starts immediately after the user passes the authentication and gets online. The accounting process does not end until the user actively gets offline. Some users, however, forget to get offline when leaving their PCs, or cannot get offline because of terminal problems. Then the users suffer certain economical losses as the accounting process continues. To more precisely determine whether a user is really online, we can preset a traffic value, so that the user is considered as not accessing the Internet and therefore directly brought offline when the user's traffic is lower than the preset value in a period of time or there is not traffic of the user at all in a period of time.

Features

Feature	Function
User Online-Status Detection	You can specify whether to detect the traffic of online users, so that a user is forced offline when the traffic of the user is lower than a preset value in a period of time.

16.3.1 User Online-Status Detection

After a user accesses the Internet, the user may forget to get offline or cannot actively get offline due to terminal faults. In this case, the user will keep being charged and therefore will suffer a certain economical loss. To protect the benefits of users on the Internet, the device provides a function to detect whether the users are really online. If the device considers that a user is not online, the device actively disconnects the user.

Working Principle

A specific detection interval is preset on the device. If a user's traffic is lower than a certain value in this interval, the device considers that the user is not using the network and therefore directly disconnects the user.

The user online-status detection function applies to only users who get online through dot1x or Web authentication.

16.3.2 User Policy Rules

After a user is successfully authenticated, the server may push some control policy names on this user. In this case, these control policy names need to be parsed by the SCC, which will convert these policy names to corresponding policy rules, and install the policies.

Working Principle

You can configure on a device the corresponding policy names, under which a speed-limit policy and filtering policy can be configured. After the user passes the authentication and the name of this policy is configured, corresponding speed-limit policy and filtering policy will take effect.

The policy needs to be configured only for users that go online through dot1x authentication or Web authentication.

16.4 Configuration

Configuration Item	Suggestions and Related Commands	
Configuring User Online-Status Detection	Optional configuration, which is used to specify whether to enable the user online-status detection function.	
	offline-detect interval threshold	Configures the parameters of the user online-status detection function.
	no offline-detect	Disables the user online-status detection function.
	default offline-detect	Restores the default user online-status detection mode.
Configuring User Policy Rules	(Optional) It is used to specify a user policy rule.	
	[no] rate-policy	Enters speed-limit policy configuration mode.
	upstream average-rate burst-rate	Configures the upstream traffic average and burst threshold.
	no upstream	Deletes the configuration for upstream traffic.
	downstream average-rate burst-rate	Configures the downstream traffic average and burst threshold.
	no downstream	Deletes the configuration for downstream traffic.
	[no] filter-policy	Enters filtering policy configuration mode.
	filter_acl	Configures the security ACL associated with the filtering policy.
	no filter_acl	Deletes the security ACL associated with the filtering policy.
	[no] service-policy	Enters user policy configuration mode.
	rate-policy apply	Configures the speed-limit policy to be used.
	no rate-policy	Deletes the speed-limit policy in use.
	filter-policy apply	Configures the filtering policy to be used.
	no filter-policy	Deletes the filtering policy in use.

16.4.1 Configuring User Online-Status Detection

Configuration Effect

After the user online-status detection function is enabled, if a user's traffic is lower than a certain threshold within the specified period of time, the device automatically disconnects the user, so as to avoid the economical loss incurred by constant charging to the user.

Precautions

It should be noted that if disconnecting zero-traffic users is configured, generally software such as 360 Security Guard will run on a user terminal by default. Then such software will send packets time and again, and the device will disconnect the user only when the user's terminal is powered off.

Configuration Method

↘ Configuring User Online-Status Detection

- Optional configuration. A user is disconnected if the user does not involve any traffic within eight hours by default.
- This configuration only works on the configured devices and does not affect other devices in the same network.

Command	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Parameter Description	*interval*: This parameter indicates the offline-detection interval. The value range is from 6 to 65535 in minutes on a switch or from 1 to 65535 in minutes on a non-switch device. The default value is 8 hours, that is, 480 minutes. *threshold*: This parameter indicates the traffic threshold. The value range is from 0 to 4294967294 in bytes. The default value is 0, indicating that the user is disconnected when no traffic of the user is detected. **no offline-detect**: Disables the user online-status detection function. **default offline-detect**: Restores the default value. In other words, an online user will be disconnected when the device detects that the user does not have any traffic within eight hours.
Defaults	8 hours
Command Mode	Global configuration mode
Usage Guide	Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specific threshold within a specific period of time. Use the **no offline-detect** command to disable the user online-status detection function, or use the **default offline-detect** command to restore the default detection mode.

Verification

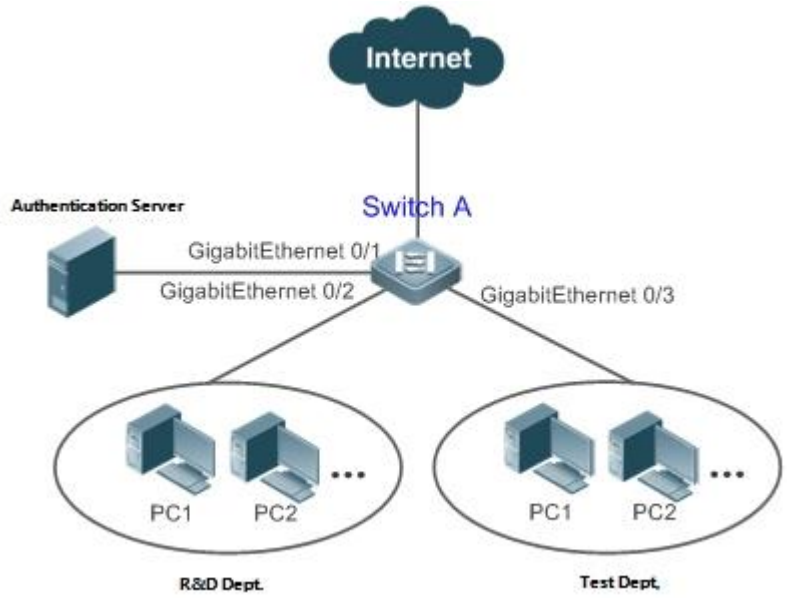
Check the user online-status detection configuration using the following method:

- After the user online-status detection function is enabled, power off the specified authenticated terminal after the corresponding user gets online. Then wait for the specified period of time, and run the online user query command associated with dot1x or Web authentication on the device to confirm that the user is already offline.

Configuration Examples

The following configuration example describes SCC-related configuration only.

Configuring User Online-Status Detection so that a User Is Disconnected if the User Does Not Have Traffic Within Five Minutes

Scenario **Figure 16-2**	
Configuration Steps	● Enable dot1x authentication on the access port Gi 0/2, and configure authentication parameters. The authentication is MAC-based. ● Configure user online-status detection so that a user is disconnected if the user does not have traffic within five minutes.
Switch A	`sw1(config)# offline-detect interval 5 threshold 0`
Verification	● Perform dot1x authentication using dot1x SU client for a PC in the R&D department, so that the PC gets online. Then power off the PC, wait for 6 minutes, and run the online user query command available with dot1x authentication on switch 1 to confirm that the user of the PC is already offline.
Switch A	`sw1(config)#show running-config | include offline-detect` `offline-detect interval 5`

16.4.2 Configuring User Policy Rules

Configuration Effect

After user policy rules are configured, you can perform speed-limit configuration for an authenticated user of specified policy names based on these policy rules.

Notes

An authentication server is required to push corresponding policy attributes. Existing policy rules support speed limit configuration and filtering configuration of wireless platforms.

Configuration Steps

Configuring User Policy Rules

- Optional.
- Configure the speed-limit policy and filtering policy first. Then configure the speed-limit policy name in the user policy rule.

The burst thresholds of upstream and downstream parameters must not be smaller than the average.

Command	**rate-policy** *name* **{downstream | upstream } average-rate** *avg-threshold* **burst-rate** *burst-threshold*
Parameter Description	***name***: Indicates the name of a speed-limit policy. ***avg-threshold***: Indicates the traffic average, in the unit of KBps. The value ranges from 8 to 261,120. ***burst-threshold***: Indicates the traffic burst threshold, in the unit of KBps. The value ranges from 8 to 261,120. The burst threshold must not be smaller than the average.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Speed-limit strategy rules must be configured first.
Command	**filter-policy** *name* **filter-acl** { *acl-name* | *acl-id* }
Parameter Description	*name*: Indicates the name of a filtering policy. *acl-name*: Indicates the name of the security ACL associated with the filtering policy. *acl-i*d: Indicates the ID of the security ACL associated with the filtering policy.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Filtering strategy rules must be configured first.
Command	**service-policy** *service-name* **rate-policy** *rate-name* **apply** **filter-policy** *filter-name* **apply**
Parameter Description	***service-name***: Indicates the name of a user policy. ***rate-name***: Indicates the name of the speed-limit policy to be used.

	filter-name: Indicates the name of the filtering policy to be used.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A speed-limit policy and filtering policy can be used user policy rules only after they are configured.

Verification

You can check the configuration effect of a policy rule as follows:

- After a speed-limit policy is configured and the user goes online through authentication, check the speed-limit policy entry corresponding to the WQoS.
- After a filtering policy is configured and the user goes online through authentication, check the ACL entry corresponding to the ACLK.

Configuration Example

Specifying the Speed-limit Policy of an Authenticated User Using a User Policy Rule

Configuration Steps	• Enable Web control on WLAN 1 and configure the corresponding user policy name on a server. • Configure a user policy rule and specify a speed-limit policy.
Switch A	`AC(config)# rate-policy user-rate` `AC(config-rate-policy)#upstream average-rate 10 burst-rate 10` `AC(config-rate-policy)#downstream average-rate 10 burst-rate 10` `AC(config)# ip access-list extended user_2000` `AC(config)# filter-policy user-filter` `AC(config-filter-policy)#filter-acl user_2000AC(config)# service-policy user-policy` `AC(config-service-policy)# rate-policy user-rate apply` `AC(config-service-policy)# filter-policy user-filter apply`
Verification	• After the user passes authentication, display upstream and downstream packets speeds.

16.5 Monitoring

Displaying

N/A

Debugging

System resources are occupied when debugging information is output. Therefore, close the debugging switch immediately after use.

Command	Function
debug scc event	Debugs the SCC running process.
debug scc user [mac | author | mac]	Debugs SCC user entries.
debug scc acl-show summary	Debugs ACLs stored in the current SCC and delivered by various services.
debug scc acl-show all	Debugs all ALCs stored in the current SCC.

17 Configuring Password Policy

17.1 Overview

The Password Policy is a password security function provided for local authentication of the device. It is configured to control users' login passwords and login states.

The following sections introduce password policy only.

Protocols and Standards

N/A

17.2 Features

Basic Concepts

Minimum Password Length

Administrators can set a minimum length for user passwords according to system security requirements. If the password input by a user is shorter than the minimum password length, the system does not allow the user to set this password but displays a prompt, asking the user to specify another password of an appropriate length.

Strong Password Detection

The less complex a password is, the more likely it is to crack the password. For example, a password that is the same as the corresponding account or a simple password that contains only characters or digits may be easily cracked. For the sake of security, administrators can enable the strong password detection function to ensure that the passwords set by users are highly complex. After the strong password detection function is enabled, a prompt will be displayed for the following types of passwords:

4. Passwords that are the same as corresponding accounts;
5. Simple passwords that contain characters or digits only.

Password Life Cycle

The password life cycle defines the validity time of a user password. When the service time of a password exceeds the life cycle, the user needs to change the password.

If the user inputs a password that has already expired during login, the system will give a prompt, indicating that the password has expired and the user needs to reset the password. If the new password input during password resetting does not meet system requirements or the new passwords consecutively input twice are not the same, the system will ask the user to input the new password once again.

Guard Against Repeated Use of Passwords

When changing the password, the user will set a new password while the old password will be recorded as the user's history records. If the new password input by the user has been used previously, the system gives an error prompt and asks the user to specify another password.

The maximum number of password history records per user can be configured. When the number of password history records of a user is greater than the maximum number configured for this user, the new password history record will overwrite the user's oldest password history record.

Storage of Encrypted Passwords

Administrators can enable the storage of encrypted passwords for security consideration. When administrators run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If administrators disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

17.3 Configuration

Configuration	Description and Command	
Configuring the Password Security Policy	⚠ Optional configuration, which is used to configure a combination of parameters related to the password security policy.	
	password policy life-cycle	Configures the password life cycle.
	password policy min-size	Configures the minimum length of user passwords.
	password policy no-repeat-times	Sets the no-repeat times of latest password configuration, so that the passwords specified in these times of latest password configuration can no longer be used in future password configuration.
	password policy strong	Enables the strong password detection function.
	service password-encryption	Sets the storage of encrypted passwords.

17.3.1 Configuring the Password Security Policy

Networking Requirements

- Provide a password security policy for local authentication of the device. Users can configure different password security policies to implement password security management.

Notes

- The configured password security policy is valid for global passwords (configured using the commands **enable password** and **enable secret**) and local user passwords (configured using the **username** *name* **password** *password* command). It is invalid for passwords in Line mode.

Configuration Steps

Configuring the Password Life Cycle

- Optional
- Perform this configuration on each device that requires the configuration of a password life cycle unless otherwise stated.

Configuring the Minimum Length of User Passwords

- Optional
- Perform this configuration on each device that requires a limit on the minimum length of user passwords unless otherwise stated.

Setting the No-Repeat Times of Latest Password Configuration

- Optional
- Perform this configuration on each device that requires a limit on the no-repeat times of latest password configuration unless otherwise stated.

Enabling the Strong Password Detection Function

- Optional
- Perform this configuration on each device that requires strong password detection unless otherwise stated.

Setting the Storage of Encrypted Passwords

- Optional
- Perform this configuration on each device that requires the storage of passwords in encrypted format unless otherwise stated.

Verification

Configure a local user on the device, and configure a valid password and an invalid password for the user.

- When you configure the valid password, the device correctly adds the password.
- When you configure the invalid password, the device displays a corresponding error log.

Related Commands

Configuring the Password Life Cycle

Command Syntax	**password policy life-cycle** *days*
Parameter Description	**life-cycle** *days*: Indicates the password life cycle in the unit of days. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	The password life cycle is used to define the validity period of user passwords. If the user logs in with a password whose service time already exceeds the life cycle, a prompt is given, asking the user to change the password.

Configuring the Minimum Length of User Passwords

Command Syntax	**password policy min-size** *length*
Parameter Description	**min-size** *length*: Indicates the minimum length of passwords. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the minimum length of passwords. If the minimum length of passwords is not configured, users can input a password of any length.

Setting the No-Repeat Times of Latest Password Configuration

Command Syntax	**password policy no-repeat-times** *times*
Parameter Description	**no-repeat-times** *times*: Indicates the no-repeat times of latest password configuration. The value range is from 1 to 31.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, all old passwords used in the several times of latest password configuration will be recorded as the user's password history records. If the new password input by the user has been used previously, the system gives an error prompt and the password modification fails. You can configure the maximum number of password history records per user. When the number of password history records of a user is greater than the maximum number configured for the user, the new password history record will overwrite the user's oldest password history record.

Enabling the Strong Password Detection Function

Command Syntax	**password policy strong**
Parameter Description	-
Command Mode	Global configuration mode

Usage Guide	After the strong password detection function is enabled, a prompt is displayed for the following types of passwords: 6. Passwords that are the same as corresponding accounts; 7. Simple passwords that contain characters or digits only.

Setting the Storage of Encrypted Passwords

Command Syntax	**service password-encryption**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Before the storage of encrypted passwords is set, all passwords used in the configuration process will be displayed and stored in plaintext format, unless the passwords are configured in cipher text format. You can enable the storage of encrypted passwords for security consideration. When you run the **show running-config** command to display configuration or run the **write** command to save configuration files, various user-set passwords are displayed in the cipher text format. If you disable the storage of encrypted passwords next time, the passwords already in cipher text format will not be restored to plaintext passwords.

Checking User-Configured Password Security Policy Information

Command Syntax	**show password policy**
Parameter Description	-
Command Mode	Privileged EXEC mode/ Global configuration mode/ Interface configuration mode
Usage Guide	Use this command to display the password security policy configured on the device.

Configuration Examples

The following configuration example describes configuration related to a password security policy.

Configuring Password Security Check on the Device

Typical Application	Assume that the following password security requirements arise in a network environment: 8. The minimum length of passwords is 8 characters; 9. The password life cycle is 90 days; 10. Passwords are stored and transmitted in cipher text format; 11. The number of no-repeat times of password history records is 3; 12. Passwords shall not be the same as user names, and shall not contain simple characters or digits only.
Configuration	● Set the minimum length of passwords to 8.

Steps	● Set the password life cycle to 90 days. ● Enable the storage of encrypted passwords. ● Set the no-repeat times of password history records to 3. ● Enable the strong password detection function.
	Ruijie# configure terminal Ruijie(config)# password policy min-size 8 Ruijie(config)# password policy life-cycle 90 Ruijie(config)# service password-encryption Ruijie(config)# password policy no-repeat-times 3 Ruijie(config)# password policy strong
Verification	When you create a user and the corresponding password after configuring the password security policy, the system will perform relevant detection according to the password security policy. ● Run the **show password policy** command to display user-configured password security policy information.
	Ruijie# show password policy Global password policy configurations: Password encryption: Enabled Password strong-check: Enabled Password min-size: Enabled (8 characters) Password life-cycle: Enabled (90 days) Password no-repeat-times: Enabled (max history record: 3)

Common Errors

- The time configured for giving a pre-warning notice about password expiry to the user is greater than the password life cycle.

17.4 Monitoring

Displaying

Command	Function
show password policy	Displays user-configured password security policy information.

18 Configuring SSH

18.1 Overview

Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user in an insecure network environment logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and plain-text password interception.

An SSH-capable device can be connected to multiple SSH clients. In addition, the device can also function as an SSH client, and allows users to set up an SSH connection with a SSH-server device. In this way, the local device can safely log in to a remote device through SSH to implement management.

Currently, a device can work as either the SSH server or an SSH client, supporting SSHv1 and SSHv2 versions. Ruijie SSH service supports both IPv4 and IPv6.

Unless otherwise specified, SSH in this document refers to SSHv2.

Protocols and Standards

- RFC 4251: The Secure Shell (SSH) Protocol Architecture
- RFC 4252: The Secure Shell (SSH) Authentication Protocol
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254: The Secure Shell (SSH) Connection Protocol
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716: The Secure Shell (SSH) Public Key File Format
- RFC 4819: Secure Shell Public Key Subsystem
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 1950: ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00: The version of the SSH Remote Login Protocol is 1.5. Comware implements the SSH server functions, but not the SSH client functions.

18.2 Applications

Application	Description
SSH Device Management	Use SSH to manage devices.
SSH Local Line Authentication	Use the local line password authentication for SSH user authentication.

Application	Description
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH user authentication.
SSH Public Key Authentication	Use the public key authentication for SSH user authentication.
SSH File Transfer	Use the Secure Copy (SCP) commands on the client to exchange data with the SSH server.

18.2.1 SSH Device Management

Scenario

You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible software includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client. Figure 18-1 shows the network topology.

Figure 18-1 Networking Topology of SSH Device Management

Deployment

Configure the SSH client as follows:

- Start the PuTTY software.
- On the **Session** option tab of PuTTY, type in the host IP address of the SSH server and SSH port number **22**, and select the connection type **SSH**.
- On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**.
- On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**.
- Click **Open** to connect to the SSH server.
- Type in the correct user name and password to enter the terminal login interface.

18.2.2 SSH Local Line Authentication

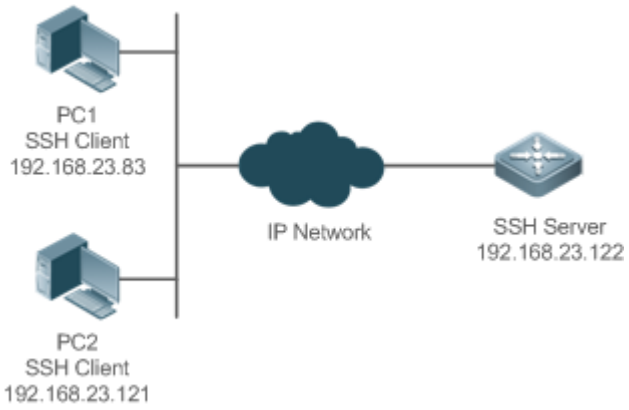
Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 18-2.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server function is enabled. The requirements are as follows:

- SSH users use the local line password authentication mode.

- Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.

Figure 18-2 Networking Topology of SSH Local Line Password Authentication



Deployment

- Configure the SSH server as follows:

13. Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2.
14. Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH clients, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses an RSA key, whereas SSHv2 adopts an RSA or DSA key.
15. Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server using this IP address. The routes from the SSH clients to the SSH server are reachable.

- Configure the SSH client as follows:

Diversified SSH client software is available, including PuTTY,Linux, and OpenSSH. This document takes PuTTY as an example to explain the method for configuring the SSH clients.

19. Open the PuTTY connection tab, and select SSHv1 for authenticated login. (The method is similar if SSHv2 is selected.)
20. Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. As the current authentication mode does not require a user name, you can type in any user name, but cannot be null. (In this example, the user name is "anyname".)

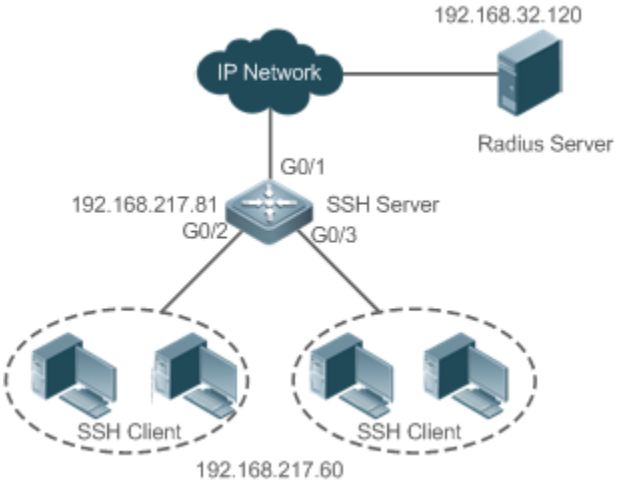
18.2.3 SSH AAA Authentication

Scenario

SSH users can use the AAA authentication mode for user authentication, as shown in Figure 18-3.To ensure security of data exchange, the PCs function as the SSH clients, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used for user login on the SSH

clients. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, it turns to the local authentication.

Figure 18-3 Networking Topology of SSH AAA Authentication



Deployment

- The routes from the SSH clients to the SSH server are reachable, and the route from the SSH server to the Radius server is also reachable.
- Configure the SSH server on the network device that functions as an SSH client.
- Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.

18.2.4 SSH Public Key Authentication

Scenario

SSH clients can use the public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 18-4.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.

Figure 18-4 Network Topology for Public Key Authentication of SSH Users

Deployment

- To implement public key authentication for the client, generate a key pair (RSA or DSA) on the client, configure the public key on the SSH server, and select the public key authentication mode.

- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash and associates the file with the SSH user name. Each user can be associated with one RSA public key and one DSA public key.

18.2.5 SSH File Transfer

Scenario

The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server, as shown in Figure 18-5.

Figure 18-5 Networking Topology of SSH File Transfer

Deployment

- Enable the SCP service on the server.
- On the client, use SCP commands to upload files to the server, or download files from the server.

18.3 Features

Basic Concepts

User Authentication Mechanism

- Password authentication

During the password authentication, a client sends a user authentication request and encrypted user name and password to the server. The server decrypts the received information, compares the decrypted information with those stored on the server, and then returns a message indicating the successful or unsuccessful authentication.

- Public key authentication

During the public key authentication, digital signature algorithms, such as RSA and DSA, are used to authenticate a client. The client sends a public key authentication request to the server. This request contains information including the user name, public key, and public key algorithm. On receiving the request, the server checks whether the public key is correct. If wrong, the server directly sends an authentication failure message. If right, the server performs digital signature authentication on the client, and returns a message indicating the successful or unsuccessful authentication.

Public key authentication is applicable only to the SSHv2 clients.

SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client undergoes the following seven stages:

- Connection setup

The server listens on Port 22 to the connection request from the client. After originating a socket initial connection request, the client sets up a TCP socket connection with the server.

- Version negotiation

If the connection is set up successfully, the server sends a version negotiation packet to the client. On receiving the packet, the client analyzes the packet and returns a selected protocol version to the server. The server analyzes the received information to determine whether version negotiation is successful.

- Key exchange and algorithm negotiation

If version negotiation is successful, key exchange and the algorithm negotiation are performed. The server and the client exchange the algorithm negotiation packet with each other, and determine the final algorithm based on their capacity. In addition, the server and the client work together to generate a session key and a session ID according to the key exchange algorithm and host key, which will be applied to subsequent user authentication, data encryption, and data decryption.

- User authentication

After the encrypted channel is set up, the client sends an authentication request to the server. The server repeatedly conducts authentication for the client until the authentication succeeds or the server shuts down the connection because the maximum number of authentication attempts is reached.

- Session request

After the successful authentication, the client sends a session request to the server. The server waits and processes the client request. After the session request is successfully processed, SSH enters the session interaction stage.

- Session interaction

After the session request is successfully processed, SSH enters the session interaction stage. Encrypted data can be transmitted and processed in both directions. The client sends a command to be executed to the client. The server decrypts, analyzes, and processes the received command, and then sends the encrypted execution result to the client. The client decrypts the execution result.

- Session ending

When the interaction between the server and the client is terminated, the socket connection disconnects, and the session ends.

Overview

Feature	Description
SSH Server	Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client.
SCP Service	After the SCP service is enabled, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

18.3.1 SSH Server

Enable the SSH server function on a network device, and you can set up a secure connection with the network device through the SSH client. You can also shut down the SSH server function to disconnect from all SSH clients.

Working Principle

For details about the working principle of the SSH server, see the "SSH Communication" in "Basic Concepts." In practice, after enabling the SSH server function, you can configure the following parameters according to the application requirements:

- Version: Configure the SSH version as SSHv1 orSSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client either when the authentication succeeds or when the authentication timeout is reached.
- Maximum number of authentication retries: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed when the maximum number of user authentication retries is reached, a message is sent, indicating the authentication failure.
- Public key authentication: The public key algorithm can be RSA or DSA. It provides a secure connection between the client and the server. The public key file on the client is associated with the user name. In addition, the public key authentication mode is configured on the client, and the corresponding private key file is specified. In this way, when the client attempts to log in to the server, public key authentication can be implemented to set up a secure connection.

Related Configuration

↘ Enabling the SSH Server

By default, the SSH server is disabled.

In global configuration mode, run the [**no**] **enable service ssh-server** command to enable or disable the SSH server.

To generate the SSH key, you also need to enable the SSH server.

↘ Specifying the SSH Version

By default, the SSH server supports both SSHv1 and SSHv2, connecting either SSHv1 clients or SSHv2 clients.

Run the **ip ssh version** command to configure the SSH version supported by the SSH server.

If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

↘ Configuring the SSH Authentication Timeout

By default, the user authentication timeout is 120s.

Run the **ip ssh time-out** command to configure the user authentication timeout of the SSH server. Use the **no** form of the command to restore the default timeout. The SSH server starts the timer after receiving a user connection request. If authentication does not succeed before the timeout is reached, authentication times out and fails.

↘ Configuring the Maximum Number of SSH Authentication Retries

By default, the maximum number of user authentication retries is 3.

Run the **ip ssh authentication-retries** command to configure the maximum number of user authentication retries on the SSH server. Use the **no** form of the command to restore the default number of user authentication retries. If authentication still does not succeed when the maximum number of user authentication retries is reached, user authentication fails.

Specifying the SSH Encryption Mode

By default, the encryption mode supported by the SSH server is Compatible, that is, supporting cipher block chaining (CBC), counter (CTR) and other encryption modes.

Run the **ip ssh cipher-mode** command to configure the encryption mode supported by the SSH server. Use the **no** form of the command to restore the default encryption mode supported by the SSH server.

Specifying the SSH Message Authentication Algorithm

By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5,SHA1,SHA1-96, and MD5-96, are supported.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by the SSH server. Use the **no** form of the command to restore the default message authentication algorithm supported by the SSH server.

Configuring Support for Diffie-Hellman(DH) Key Exchange Algorithm on the SSH Server

By default, Ruijie's SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for keyexchange while the SSHv1 server support none. Run the **ip ssh key-exchange** command to configure support for Diffie-Hellman on the SSH server. Use the **no ip ssh key-exchange** command to restore the default setting.

Setting A Monitoring Port ID for the SSH Server

The default port ID is 22.

Run the **ip ssh port** command to set a monitoring port ID for the SSH server. Use either the **no ip ssh port** command or the **ip ssh port 22** command to restore the default setting.

Enabling the Public Key Authentication on the SSH Server

Run the **ip ssh peer** command to associate the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

18.3.2 SCP Service

The SSH server provides the SCP service to implement secure file transfer between the server and the client.

Working Principle

- SCP is a protocol that supports online file transfer. It runs on Port 22 based on the BSC RCP protocol, whereas RCP provides the encryption and authentication functions based on the SSH protocol. RCP implements file transfer, and SSH implements authentication and encryption.

- Assume that the SCP service is enabled on the server. When you use an SCP client to upload or download files, the SCP client first analyzes the command parameters, sets up a connection with a remote server, and starts another SCP process based on this connection. This process may run in source or sink mode. (The process running in source mode is the data provider. The process running in sink mode is the destination of data.) The process running in source mode reads and sends files to the peer end through the SSH connection. The process running in sink mode receives files through the SSH connection.

Related Configuration

Enabling the SCP Server

By default, the SCP server function is disabled.

Run the **ip scp server enable** command to enable SCP server function on a network device.

Configuring the Transmission Path for Files of the SCP Server

The default transmission path is **flash:/**.

Run the **ip scp server topdir {flash:/***path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}** command to configure the transmission path to upload files to or download files from the SCP server.

18.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	⚠ It is mandatory to enable the SSH server.	
	enable service ssh-server	Enables the SSH server.
	disconnect ssh[**vty**] *session-id*	Disconnects an established SSH session.
	crypto key generate {**rsa**|**dsa**}	Generates an SSH key.
	ip ssh version {**1**|**2**}	Specifies the SSH version.
	ip ssh time-out *time*	Configures the SSH authentication timeout.
	ip ssh authentication-retries *retry times*	Configures the maximum number of SSH authentication retries.
	Ip ssh cipher-mode{**cbc** | **ctr** | **others** }	Specifies the SSH encryption mode.
	Ip ssh hmac-algorithm{**md5** | **md5-96** | **sha1** | **sha1-96**}	Specifies the SSH message authentication algorithm.
	ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }	Configures support for Diffie-Hellman on the SSH server.
	ip ssh port *port*	Sets a monitoring port ID for the SSH server.
	ip ssh peer *test* **public-key rsa flash** *:rsa.pub*	Associates an RSA public key file with a user.

Configuration	Description and Command	
	ip ssh peer *test* **public-key dsa flash**:*dsa.pub*	Associates a DSA public key file with a user.
Configuring the SCP Service	⚠ Mandatory.	
	ip scp server enable	Enables the SCP server.
	ip scp server topdir {flash:/*path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}**	Configures the transmission path for files of the SCP server

18.4.1 Configuring the SSH Server

Configuration Effect

- Enable the SSH server function on a network device so that you can set up a secure connection with a remote network device through the SSH client. All interactive data is encrypted before transmitted, featuring authentication and security.
- You can use diversified SSH user authentications modes, including local line password authentication, AAA authentication, and public key authentication.
- You can generate or delete an SSH key.
- You can specify the SSH version.
- You can configure the SSH authentication timeout.
- You can configure the maximum number of SSH authentication retries.
- You can specify the SSH encryption mode.
- You can specify the SSH message authentication algorithm.
- You can specify ACL filtering of the SSH server.

Notes

- The precondition of configuring a device as the SSH server is that communication is smooth on the network that the device resides, and the administrator can access the device management interface to configure related parameters.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.
- The SSH module does not support hot standby. Therefore, for products that supports hot standby on the supervisor modules, if no SSH key file exist on the new active module after failover, you must run the **crypto key generate** command to re-generate a key before using SSH.

Configuration Steps

↘ Enabling the SSH Server

- Mandatory.

- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and generate an SSH key so that the SSH server state changes to ENABLE.

Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, connecting either SSHv1 or SSHv2clients. If only SSHv1 or SSHv2 is configured, only the SSH client of the configured version can be connected to the SSH server.

Configuring the SSH Authentication Timeout

- Optional.
- By default, the SSH authentication timeout is 120s. You can configure the user authentication timeout as required. The value ranges from 1 to 120. The unit is second.

Configuring the Maximum Number of SSH Authentication Retries

- Optional.
- Configure the maximum number of SSH authentication retries to prevent illegal behaviors such as malicious guessing. By default, the maximum number of SSH authentication retries is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum number of retries as required. The value ranges from 0 to 5.

Specifying the SSH Encryption Mode

- Optional.
- Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is Compatible, that is, supporting CBC, CTR and other encryption modes.

Specifying the SSH Message Authentication Algorithm

- Optional.
- Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For the SSHv1, no algorithm is supported; (2) For the SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.

Enabling the Public Key Authentication for SSH Users

- Optional.
- Only SSHv2 supports authentication based on the public key. This configuration associates a public key file on the client with a user name. When a client is authenticated upon login, a public key file is specified based on the user name.

Verification

- Run the **show ip ssh** command to display the current SSH version, port number, encryption mode, message authentication algorithm, authentication timeout, and maximum number of authentication retries of the SSH server.

- Run the **show crypto key mypubkey** command to display the public information of the public key to verify whether the key has been generated.
- Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Related Commands

Enabling the SSH Server

Command	**enable service ssh-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To disable the SSH server, run the **no enable service ssh-server** command in global configuration mode. After this command is executed, the SSH server state changes to DISABLE.

Disconnecting an Established SSH Session

Command	**disconnect ssh**[**vty**] *session-id*
Parameter Description	**vty:** Indicates an established virtual teletype terminal (VTY) session. *session-id*: Indicates the ID of the established SSH session. The value ranges from 0 to 35.
Command Mode	Privileged EXEC mode
Usage Guide	Specify an SSH session ID to disconnect the established SSH session. Alternatively, specify a VTY session ID to disconnect a specified SSH session. Only an SSH session can be disconnected.

Generating an SSH Key

Command	**crypto key generate** {**rsa**|**dsa**}
Parameter Description	**rsa:** Generates an RSA key. **dsa:** Generates a DSA key.
Command Mode	Global configuration mode
Usage Guide	The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. If an RSA key is generated, both SSHv1 and SSHv2 are supported. If only a DSA key is generated, only SSHv2 can use the key.

Specifying the SSH Version

Command	**ip ssh version** {**1**|**2**}
Parameter	**1:** Indicates that the SSH server only receives the connection requests sent by SSHv1 clients.

Description	**2:** Indicates that the SSH server only receives the connection requests sent by SSHv2 clients.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh version** command to restore the default settings. By default, the SSH server supports both SSHv1 and SSHv2.

Configuring the SSH Authentication Timeout

Command	**ip ssh time-out** *time*
Parameter Description	*time***:** Indicates the SSH authentication timeout. The value ranges from 1 to 120. The unit is second.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh time-out** command to restore the default SSH authentication timeout, which is 120s.

Configuring the Maximum Number of SSH Authentication Retries

Command	**ip ssh authentication-retries** *retry times*
Parameter Description	*retry times***:** Indicates the maximum number of user authentication retries. The value ranges from 0 to 5.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh authentication-retries** command to restore the default number of user authentication retries, which is 3.

Specifying the SSH Encryption Mode

Command	**ip ssh cipher-mode**{**cbc** | **ctr** | **others** }
Parameter Description	**cbc:** Sets the encryption mode supported by the SSH server to the CBC mode. Corresponding algorithms include DES-CBC,3DES-CBC,AES-128-CBC,AES-192-CBC,AES-256-CBC, and Blowfish-CBC. **ctr:** Sets the encryption mode supported by the SSH server to the CTR mode. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR. **others:** Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the encryption mode supported by the SSH server. On Ruijie devices, the SSHv1 server supports the DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; the SSHv2 server supports the AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4 encryption algorithms. These algorithms can be grouped into three encryption modes: CBC, CTR, and others. As the cryptography continuously develops, it is approved that encryption algorithms in the CBC and others modes can be decrypted in a limited period of time. Therefore, organizations or companies that have high security requirements can set the encryption mode supported by the SSH server to CTR to increase the

	security level of the SSH server.

Specifying the SSH Message Authentication Algorithm

Command	**ip ssh hmac-algorithm**{**md5** | **md5-96** | **sha1** | **sha1-96**}
Parameter Description	**md5:** Indicates that the message authentication algorithm supported by the SSH server is MD5. **md5-96:** Indicates that the message authentication algorithm supported by the SSH server is MD5-96. **sha1:** Indicates that the message authentication algorithm supported by the SSH server is SHA1. **sha1-96:** Indicates that the message authentication algorithm supported by the SSH server is SHA1-96.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the message authentication algorithm supported by the SSH server. On Ruijie devices, the SSHv1 server does support any message authentication algorithm; the SSHv2 server supports the MD5**,** SHA1**,** SHA1-96**, and** MD5-96 message authentication algorithms. You can select message authentication algorithms supported by the SSH server as required.

Configuring Support for DH Key Exchange Algorithm on the SSH Server

Command	**ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }**
Parameter Description	**dh_group_exchange_sha1**: Indicates configuration of diffie-hellman-group-exchange-sha1 for keyexchange. The key has 2,048 bytes, which cannot be edited. **dh_group14_sha1**: Indicates configuration of diffie-hellman-group14-sha1 for keyexchange. The key has 2,048 bytes. **dh_group1_sha1**: Indicates configuration of diffie-hellman-group1-sha1 for keyexchange. The key has 1,024 bytes.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a DH key exchange method on the SSH. Ruijie's SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for keyexchange.

Setting A Monitoring Port ID for the SSH Server

Command	**ip ssh port** *port*
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value ranges from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use either the **no ip ssh port** or the **ip ssh port 22** to restore the monitoring port ID of the SSH server to the default value.

Configuring RSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key rsaflash**:*rsa.pub*

Parameter Description	*test*: Indicates the user name. **rsa:** Indicates that the public key type is RSA. *rsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the RSA public key file associated with user *test*. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuring DSA Public Key Authentication

Command	**ip ssh peer** *test* **public-key dsaflash**:*dsa.pub*
Parameter Description	*test*: Indicates the user name. **dsa**: Indicates that the public key type is DSA. *dsa.pub*: Indicates the name of a public key file.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the DSA key file associated with user **test**. Only SSHv2 supports authentication based on the public key. This command associates the public key file on the client with the user name. When the client is authenticated upon login, a public key file is specified based on the user name.

Configuration Example

The following configuration examples describe only configurations related to SSH.

Generating a Public Key on the SSH Server

Configuration Steps	● Run the **crypto key generate { rsa | dsa }** command to generate a RSA public key for the server.

SSH Server	Ruijie#configure terminal Ruijie(config)# crypto key generate rsa Choose the size of the rsa key modulus in the range of 512 to 2048 and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: ● If the generation of the RSA key is successful, the following information is displayed: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] ● If the generation of the RSA key fails, the following information is displayed: % Generating 512 bit RSA1 keys ...[fail] % Generating 512 bit RSA keys ...[fail]
Verification	● Run the **show crypto key mypubkey rsa** command to display the public information about the RSA key. If the public information about the RSA key exists, the RSA key has been generated.
SSH Server	Ruijie(config)#show crypto key mypubkey rsa % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU 8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j 0dKBcCfN tr0r/CT+ cs5tlGKV S0ICGifz oB+pYaE= % Key pair was generated at: 1:49:47 UTC Jan 4 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data:

	AAAAAwEAAQAAAHJfLwKnzOgO F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQ0Q80 sISgIfZ9 8o5No3Zz MPM0LnQR G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEYXCFaaxU=

Specifying the SSH Version

Configuration Steps	● Run the **ip ssh version** { **1 | 2** } command to set the version supported by the SSH server to SSHv2.
SSH Server	Ruijie#configure terminal Ruijie(config)#ip ssh version 2
Verification	● Run the **show ip ssh** command to display the SSH version currently supported by the SSH server.
SSH Server	Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the SSH Authentication Timeout

Configuration Steps	● Run the **ip ssh time-out** *time* command to set the SSH authentication timeout to 100s.
SSH Server	Ruijie#configure terminal Ruijie(config)#ip sshtime-out100
Verification	● Run the **show ip ssh** command to display the configured SSH authentication timeout.
SSH Server	Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 100 secs

	Authentication retries: 3 SSH SCP Server: disabled

Configuring the Maximum Number of SSH Authentication Retries

Configuration Steps	● Run the **ip ssh authentication-retries** *retry times* command to set the maximum number of user authentication retries on the SSH server to 2.
SSH Server	Ruijie#configure terminal Ruijie(config)#ip ssh authentication-retries 2
Verification	● Run the **show ip ssh** command to display the configured maximum number of authentication retries.
SSH Server	Ruijie(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 2 SSH SCP Server: disabled

Specifying the SSH Encryption Mode

Configuration Steps	● Run the **ip ssh cipher-mode** {**cbc** | **ctr** | **others** }command to set the encryption mode supported by the SSH server to CTR.
SSH Server	Ruijie#configure terminal Ruijie(config)# ip ssh cipher-mode ctr
Verification	● Select the CTR encryption mode on the SSH client, and verify whether you can successfully log in to the SSH server from the SSH client.

Specifying the SSH Message Authentication Algorithm

Configuration Steps	● Run the **ip ssh hmac-algorithm** {**md5** | **md5-96** | **sha1** | **sha1-96** } command to set the message authentication algorithm supported by the SSH server to SHA1.
SSH Server	Ruijie#configure terminal Ruijie(config)# ip ssh hmac-algorithmsha1
Verification	● Select the SHA1 message authentication algorithm on the SSH client, and verify whether you can

	successfully log in to the SSH server from the SSH client.

Configuring Support for DH Key Exchange Algorithm on the SSH Server

Configuration Steps	● Run the **ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }**command to configure a key exchange method on the SSH server.
SSH Server	Ruijie# configure terminal Ruijie(config)# ip ssh key-exchange dh_group14_sha1
Verification	● Choose diffie-hellman-group14-sha1 on the client terminal and check if successful login is performed.

Setting A Monitoring Port ID for the SSH Server

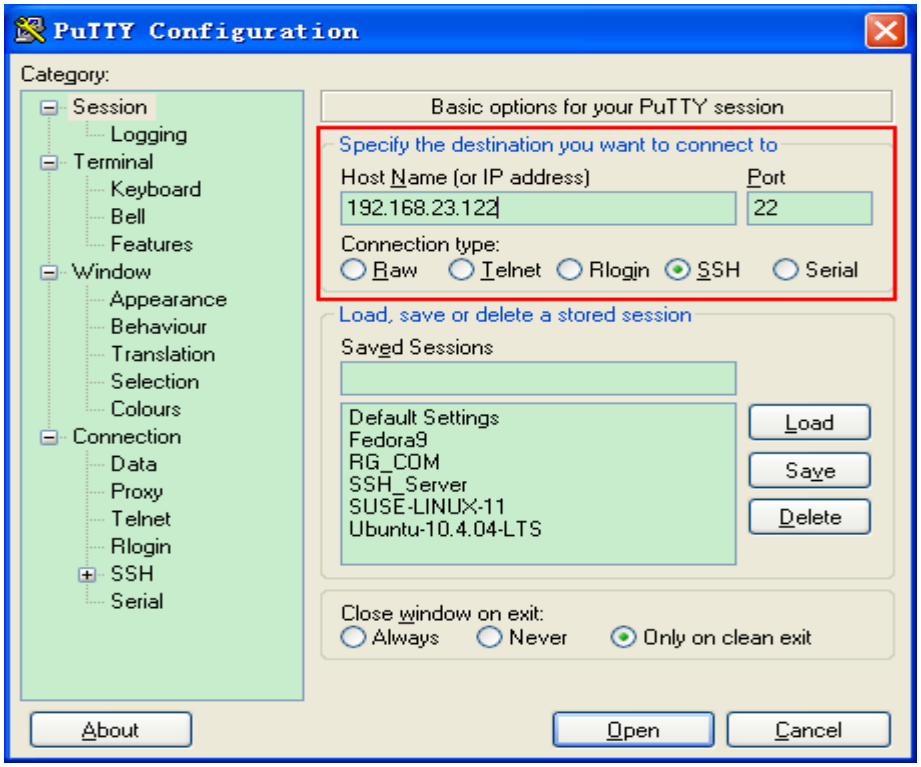
Command	**ip ssh port** *port*
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value ranges from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use either the **no ip ssh port** or the **ip ssh port 22** to restore the monitoring port ID of the SSH server to the default value.

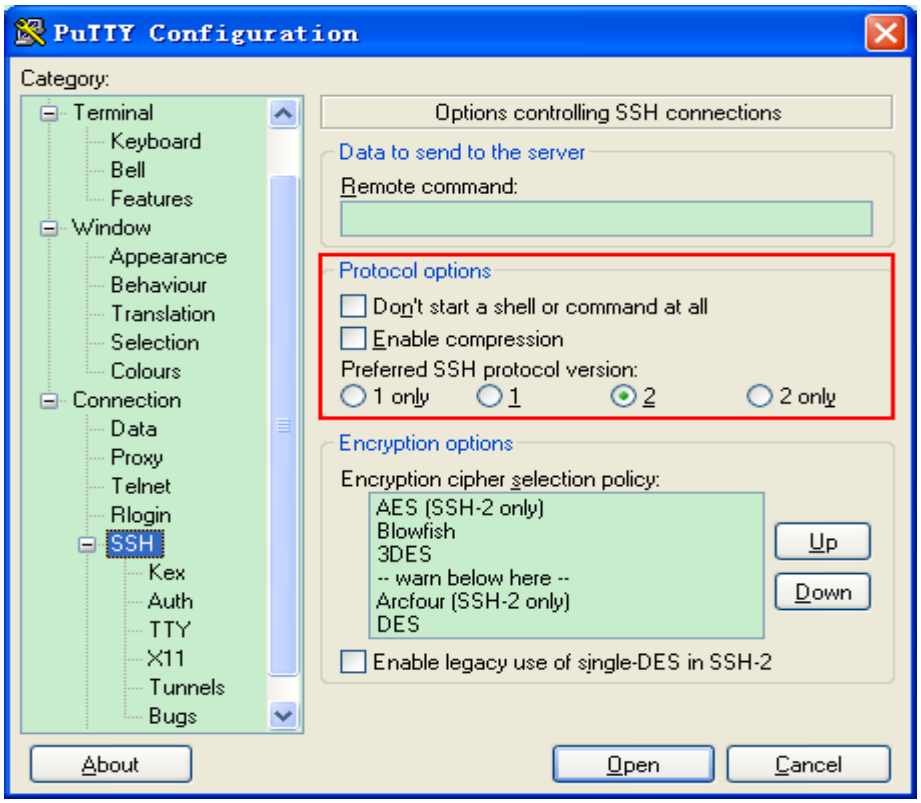
Configuring the Public Key Authentication

Configuration Steps	● Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa**}*filename* command to associate a public key file of the client with a user name. When the client is authenticated upon login, a public key file (for example, RSA) is specified based on the user name.
SSH Server	Ruijie#configure terminal Ruijie(config)# ip ssh peer test public-key rsaflash:rsa.pub
Verification	● Configure the public key authentication login mode on the SSH client and specify the private key file. Check whether you can successfully log in to the SSH server from the SSH client. If yes, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

Configuring SSH Device Management

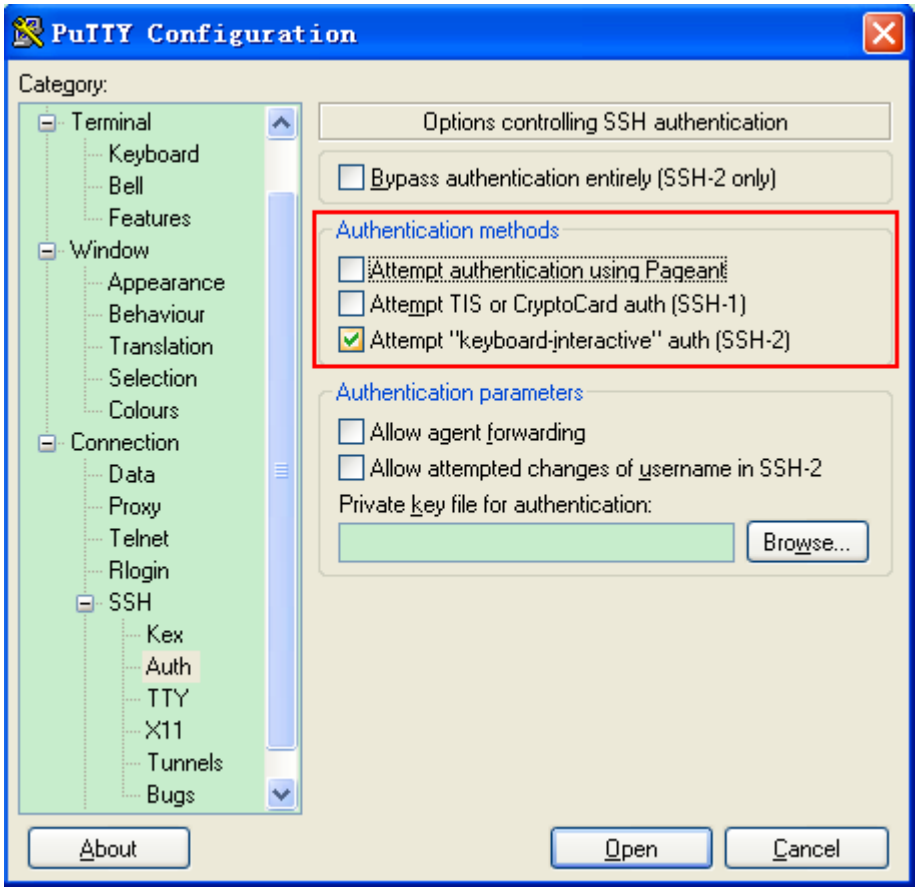
Scenario Figure18-6	 You can use SSH to manage devices on the precondition that the SSH server function is enabled. By default, this function is disabled. The Telnet component that comes with the Windows does not support SSH. Therefore, a third-party client software must be used. Currently, well-compatible client software

	includes PuTTY, Linux, and SecureCRT. The following takes the PuTTY as an example to introduce the configurations of the SSH client.
Configuration Steps	● Start the PuTTY software. ● On the **Session** option tab of PuTTY, type in the host IP address **192.168.23.122** and SSH port number **22**, and select the connection type **SSH**. ● On the **SSH** option tab of PuTTY, select the preferred SSH protocol version **2**. ● On the **SSH authentication** option tab of PuTTY, select the authentication method **Attempt "keyboard-interactive" auth**. ● Click **Open** to connect to the SSH server. ● Type in the correct user name and password to enter the terminal login interface.
SSH Client	Figure 18-6  **Host Name (or IP address)** indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, the default ID of the port listened by SSH. **Connection type** is **SSH**. Figure 18-7



As shown in Figure 18-7, select **2** as the preferred SSH protocol version in the **Protocol options** pane because SSHv2 is used for login.

Figure 18-8



As shown in Figure 18-8, select **Attempt "keyboard-interactive" auth** as the authentication method to support authentication based on the user name and password.

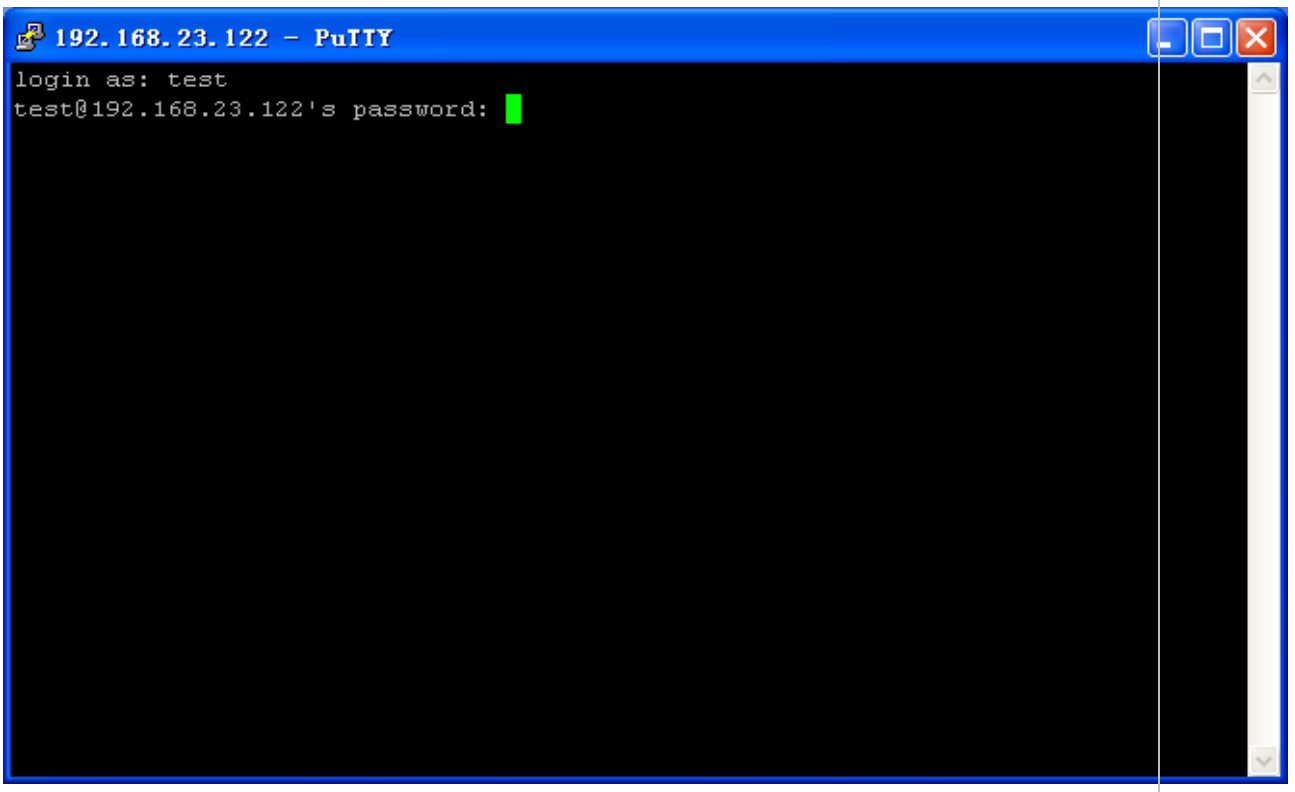
Then, click **Open** to connect to the configured server host, as shown in Figure 18-9.

Figure 18-9

The **PuTTY Security Alert** box indicates that you are logging in to the client of the server 192.168.23.122, and asks you whether to receive the key sent from the server.

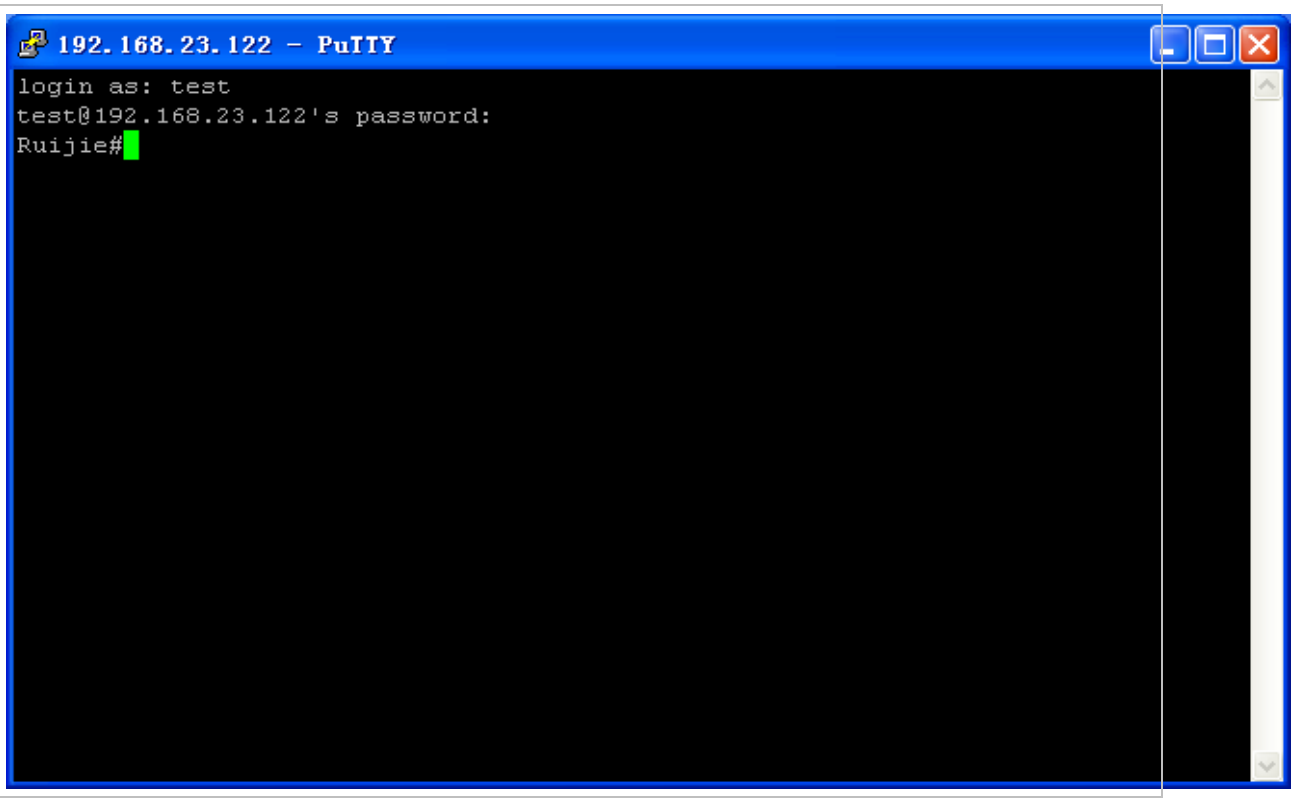
If you select **Yes**, a login dialog box is displayed, as shown in Figure 18-10.

Figure 18-10



Type in the correct user name and password, and you can log in to the SSH terminal interface, as shown in Figure 18-11.

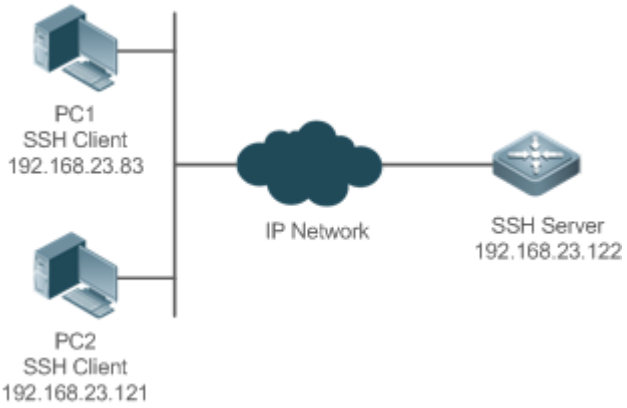
Figure 18-11



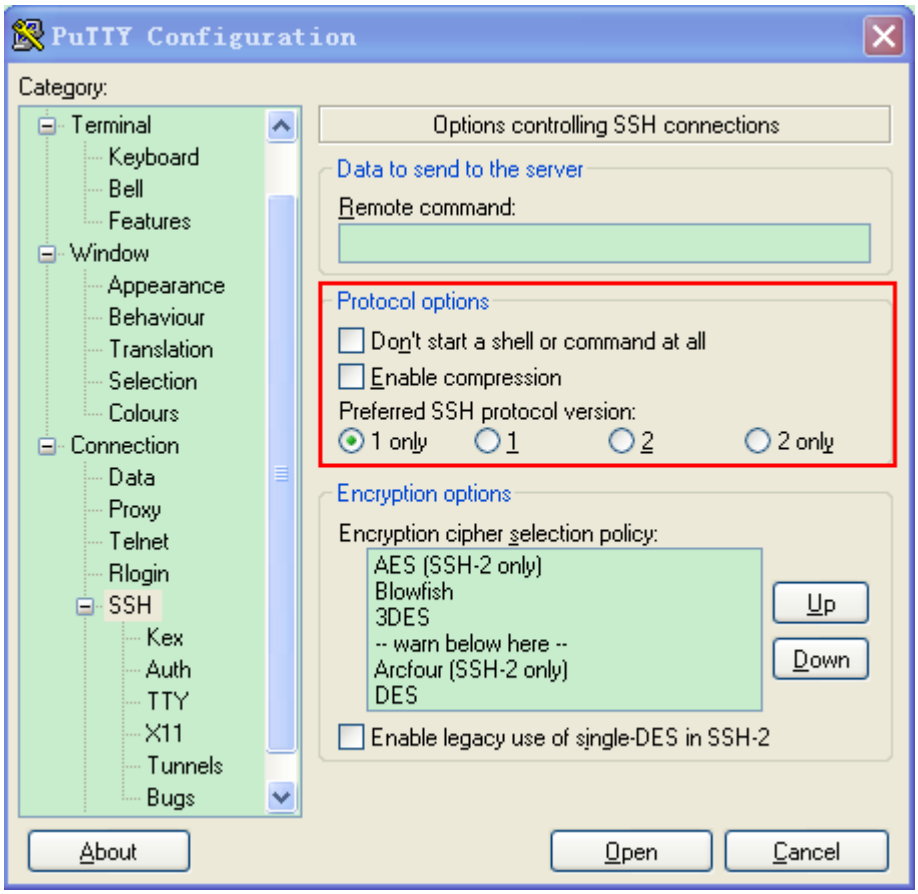
Verification	● Run the **show ip ssh** command to display the configurations that are currently effective on the SSH server. ● Run the **show ssh** command to display information about every SSH connection that has been established.

```
Ruijie#show ip ssh
SSH Enable - version 1.99
SSH Port:                22
SSH Cipher Mode:         cbc,ctr,others
SSH HMAC Algorithm:      md5-96,md5,sha1-96,sha1
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server:          disabled
Ruijie#show ssh
Connection Version Encryption       Hmac         State           Username
         0     2.0 aes256-cbc       hmac-sha1    Session started test
```

Configuring SSH Local Line Authentication

Scenario **Figure** 18-12	 SSH users can use the local line password for user authentication, as shown in Figure 18-12.To ensure security of data exchange, PC 1 and PC 2 function as the SSH clients, and use the SSH protocol to log in to the network device where the SSH server is enabled. The requirements are as follows: ● SSH users use the local line password authentication mode. ● Five lines, including Line 0 to Line 4, are activated concurrently. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Any user name can be used.
Configuration Steps	Configure the SSH server as follows: ● Enable the SSH server function globally. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. ● Configure the key. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted plain text with the password stored on the server, and returns a message indicating the successful or unsuccessful authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ● Configure the IP address of the FastEthernet 0/1 interface on the SSH server. The SSH client is connected to the SSH server based on this IP address. The route from the SSH client to the SSH server is reachable. Configure the SSH client as follows: ● Diversified SSH client software is available, including PuTTY, Linux, and SecureCRT. This document takes PuTTY as an example to explain the method for configuring the SSH client. For details about the configuration method, see "Configuration Steps."
SSH Server	Before configuring SSH-related function, ensure that the route from the SSH user to the network segment of the SSH server is reachable. The interface IP address configurations are shown in Figure 18-13. The detailed procedures for configuring IP addresses and routes are omitted. Ruijie(config)# enable service ssh-server Ruijie(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your

	Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Ruijie(config)#interface fastEthernet0/1 Ruijie(config-if-fastEthernet0/1)#ip address 192.168.23.122 255.255.255.0 Ruijie(config-if-fastEthernet0/1)#exit Ruijie(config)#line vty 0 Ruijie(config-line)#password passzero Ruijie(config-line)#privilege level 15 Ruijie(config-line)#login Ruijie(config-line)#exit Ruijie(config)#line vty1 4 Ruijie(config-line)#password pass Ruijie(config-line)#privilege level 15 Ruijie(config-line)#login Ruijie(config-line)#exit
SSH Client(PC1/ PC2)	Figure 18-13

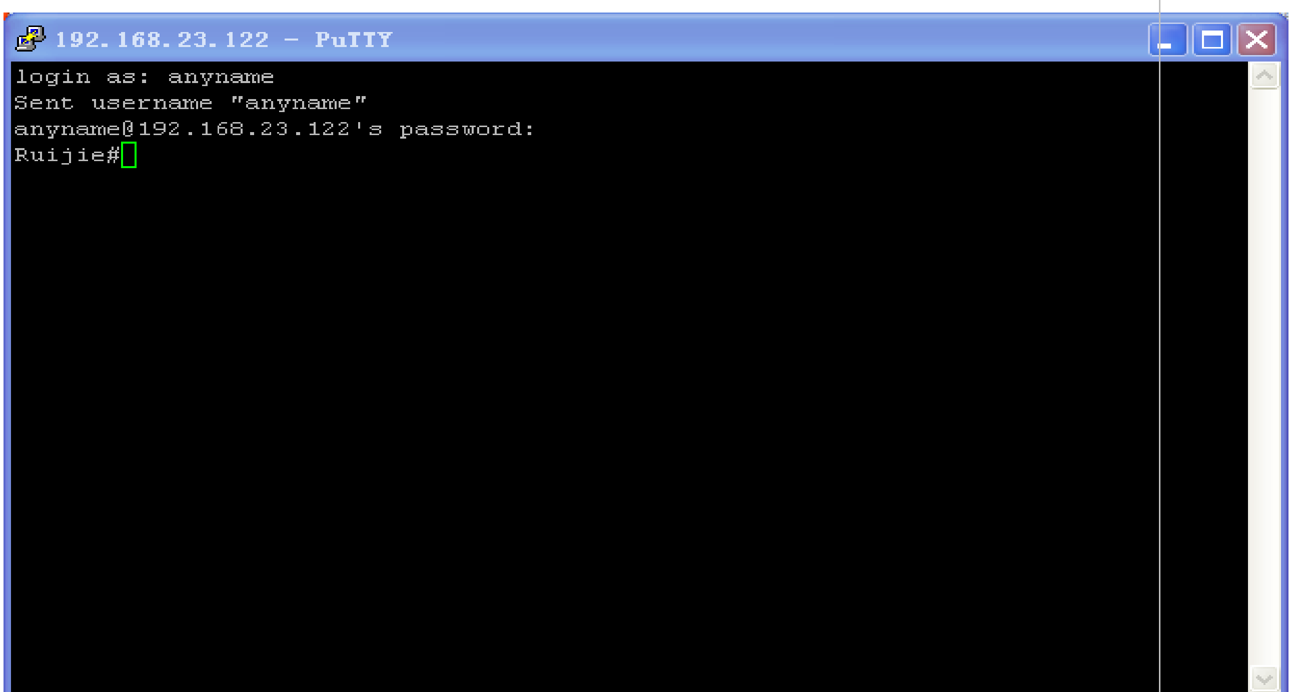


Set the IP address and port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22 (For details about the configuration method, see "Configuring SSH Device Management."). Click **Open** to start the SSH server. As the current authentication mode does not require a user name, you can type in any user name, but cannot leave the user name unspecified. (In this example, the user name is "anyname".)

Verification	● Run the **show running-config** command to display the current configurations. ● Verify that the SSH client configurations are correct.
SSH Server	Ruijie#show running-config Building configuration... ! enable secret 5 1eyy2$xs28FDw4s2q0tx97 enable service ssh-server ! interface fastEthernet0/1 ip address 192.168.23.122 255.255.255.0

<table>
<tr><td></td><td>!
line vty 0
privilege level 15
  login
  password passzero
line vty 1 4
privilege level 15
  login
  password pass
!
end</td></tr>
<tr><td>SSH Client</td><td>Set up a connection, and enter the correct password. The login password is "passzero" for Line 0 and "pass" for the remaining lines. Then, the SSH server operation interface is displayed, as shown in Figure 18-14.

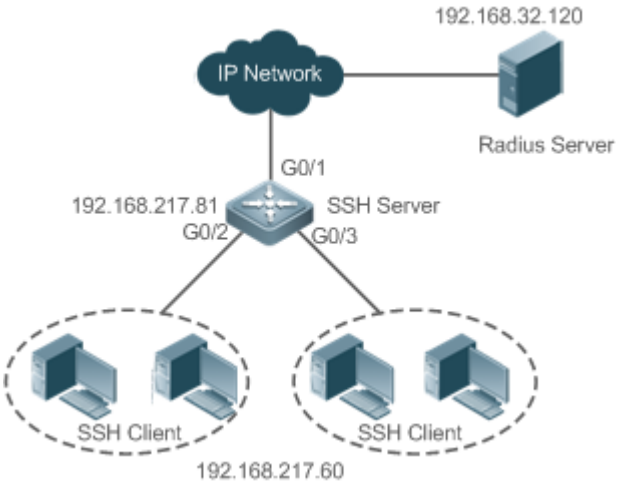
Figure 18-14

Ruijie#show users
Line User Host(s) Idle Location
---------------- ------------ -------------------- ---------- ------------------
* 0 con 0 --- idle 00:00:00 ---</td></tr>
</table>

	1 vty 0	---	idle	00:08:02	192.168.23.83
	2 vty 1	---	idle	00:00:58	192.168.23.121

Configuring AAA Authentication of SSH Users

Scenario **Figure** 18-15	 SSH users can use the AAA authentication mode for user authentication, as shown in Figure 18-15.To ensure security of data exchange, the PC functions as the SSH client, and uses the SSH protocol to log in to the network device where the SSH server is enabled. To better perform security management, the AAA authentication mode is used on the user login interface of the SSH client. Two authentication methods, including Radius server authentication and local authentication, are provided in the AAA authentication method list to ensure reliability. The Radius server authentication method is preferred. If the Radius server does not respond, select the local authentication method.
Configuration Steps	● The route from the SSH client to the SSH server is reachable, and the route from the SSH server to the Radius server is also reachable. ● Configure the SSH server on the network device. The configuration method is already described in the previous example, and therefore omitted here. ● Configure the AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define the identity authentication and types, and applied to a specified service or interface.
SSH Server	Ruijie(config)# enable service ssh-server Ruijie(config)#crypto key generate rsa % You already have RSA keys. % Do you really want to replace them? [yes/no]: Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take

	a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA1 keys ...[ok] % Generating 512 bit RSA keys ...[ok] Ruijie(config)#crypto key generate dsa Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit DSA keys ...[ok] Ruijie(config)#interface gigabitEthernet1/1 Ruijie(config-if-gigabitEthernet1/1)#ip address 192.168.217.81 255.255.255.0 Ruijie(config-if-gigabitEthernet1/1)#exit Ruijie#configure terminal Ruijie(config)#aaa new-model Ruijie(config)#radius-server host 192.168.32.120 Ruijie(config)#radius-server key aaaradius Ruijie(config)#aaa authentication login methodgroup radius local Ruijie(config)#line vty 0 4 Ruijie(config-line)#login authentication method Ruijie(config-line)#exit Ruijie(config)#username user1 privilege 1 password 111 Ruijie(config)#username user2 privilege 10 password 222 Ruijie(config)#username user3 privilege 15 password 333 Ruijie(config)#enable secret w
Verification	● Run the **show running-config** command to display the current configurations. ● This example assumes that the SAM server is used. ● Set up a remote SSH connection on the PC. ● Check the login user.
	Ruijie#show run aaa new-model

```
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet1/1
 no ip proxy-arp
ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
End
```

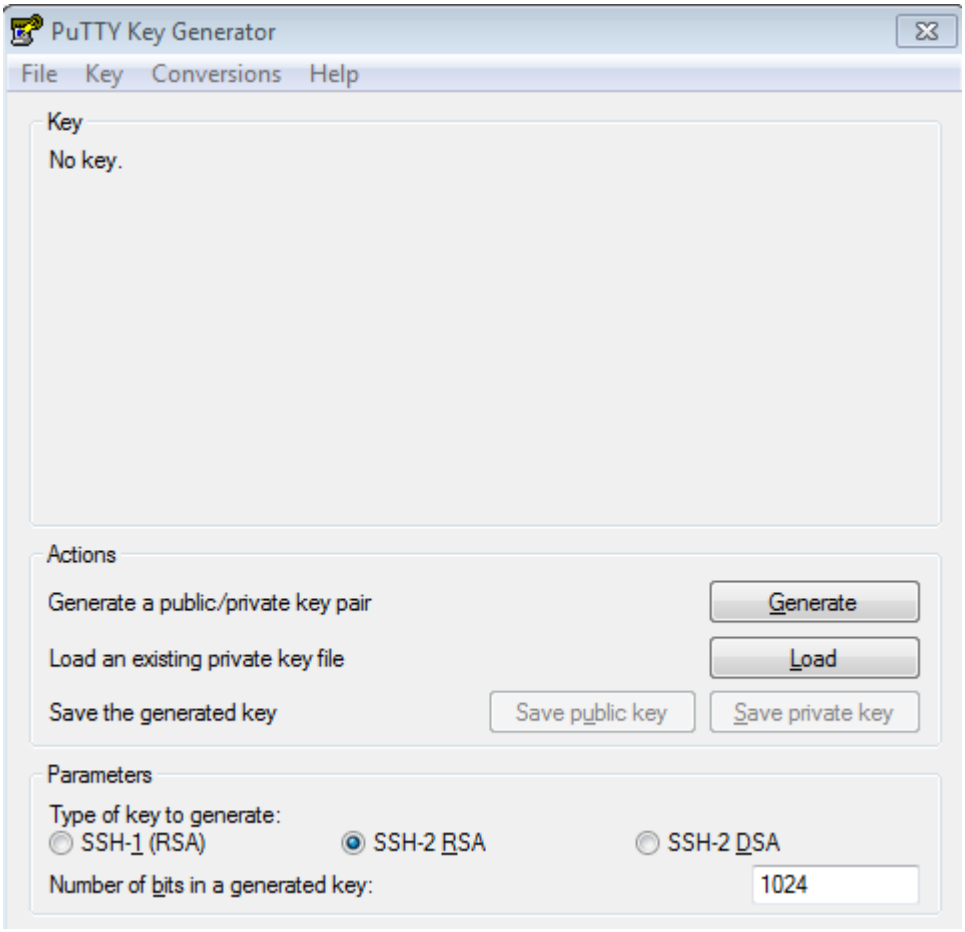
On the SSH client, choose **System Management**>**Device Management**, and add the device IP address **192.168.217.81** and the device key **aaaradius**.
Choose **Security Management**>**Device Management Rights**, and set the rights of the login user.
Choose **Security Management**>**Device Administrator**, and add the user name **user** and password **pass**.
Configure the SSH client and set up a connection to the SSH server. For details, see the previous example.
Type in the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
Ruijie#show users
```

	Line User Host(s) Idle Location 0 con 0 idle 00:00:31 * 1 vty 0 user idle 00:00:33 192.168.217.60

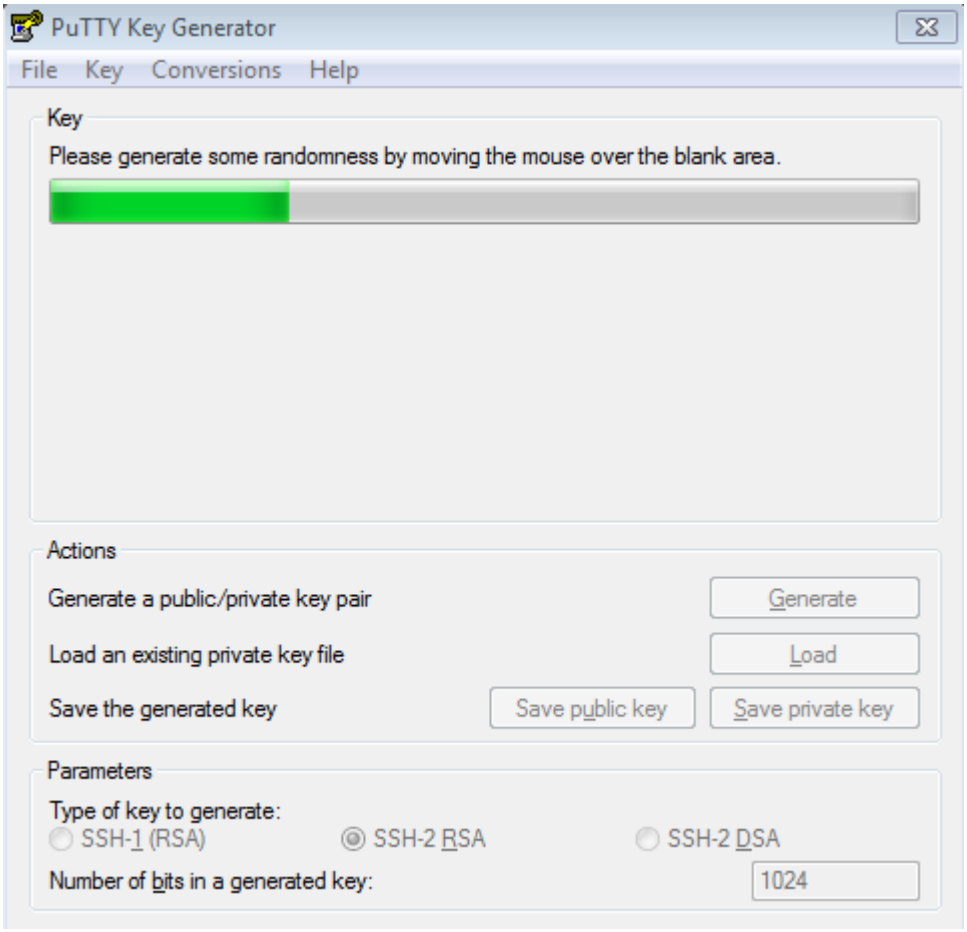
Configuring Public Key Authentication of SSH Users

Scenario **Figure** 18-16	 SSH users can use the public key for user authentication, and the public key algorithm is RSA or DSA, as shown in Figure 18-16.SSH is configured on the client so that a secure connection is set up between the SSH client and the SSH server.
Configuration Steps	● To implement public key authentication on the client, generate a key pair (for example, RSA key) on the client, place the public key on the SSH server, and select the public key authentication mode. After the key pair is generated on the client, you must save and upload the public key file to the server and complete the server-related settings before you can continue to configure the client and connect the client with the server. ● After the key is generated on the client, copy the public key file from the client to the flash of the SSH server, and associate the file with an SSH user name. A user can be associated with one RSA public key and one DSA public key.
SSH Client	Run the **puttygen.exe** software on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 18-17. Figure 18-17



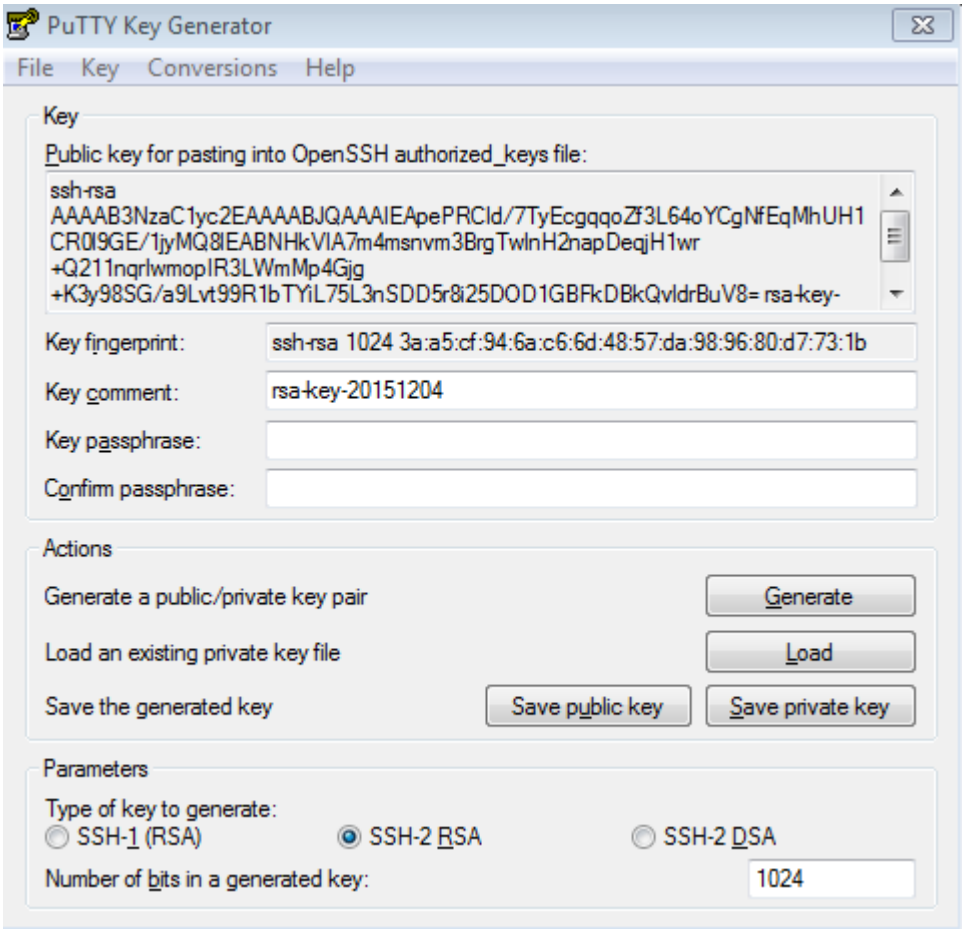
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 18-18.

Figure 18-18



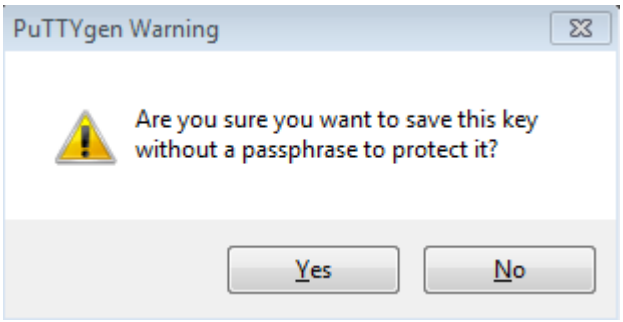
To ensure security of the RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 18-19



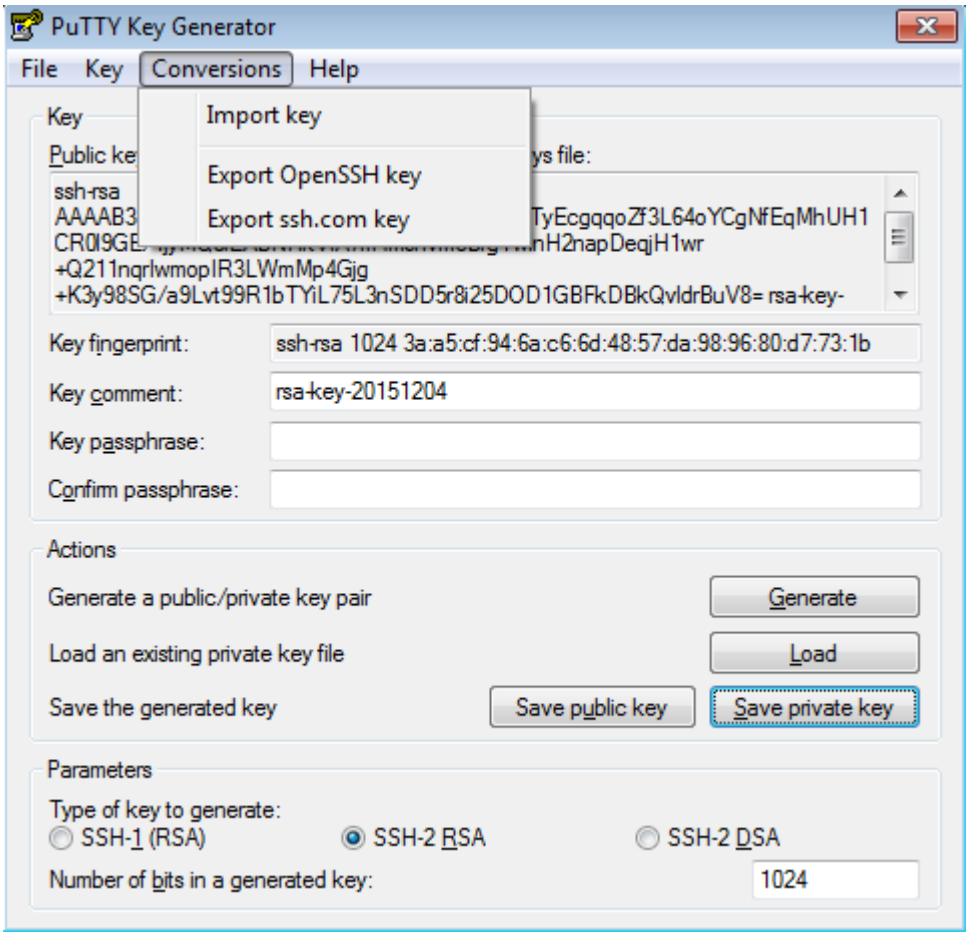
After the key pair is generated, click **Save public key**, type in the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following prompt box is displayed. Select **Yes**, type in the public key name **test_private**, and click **Save**.

Figure 18-20

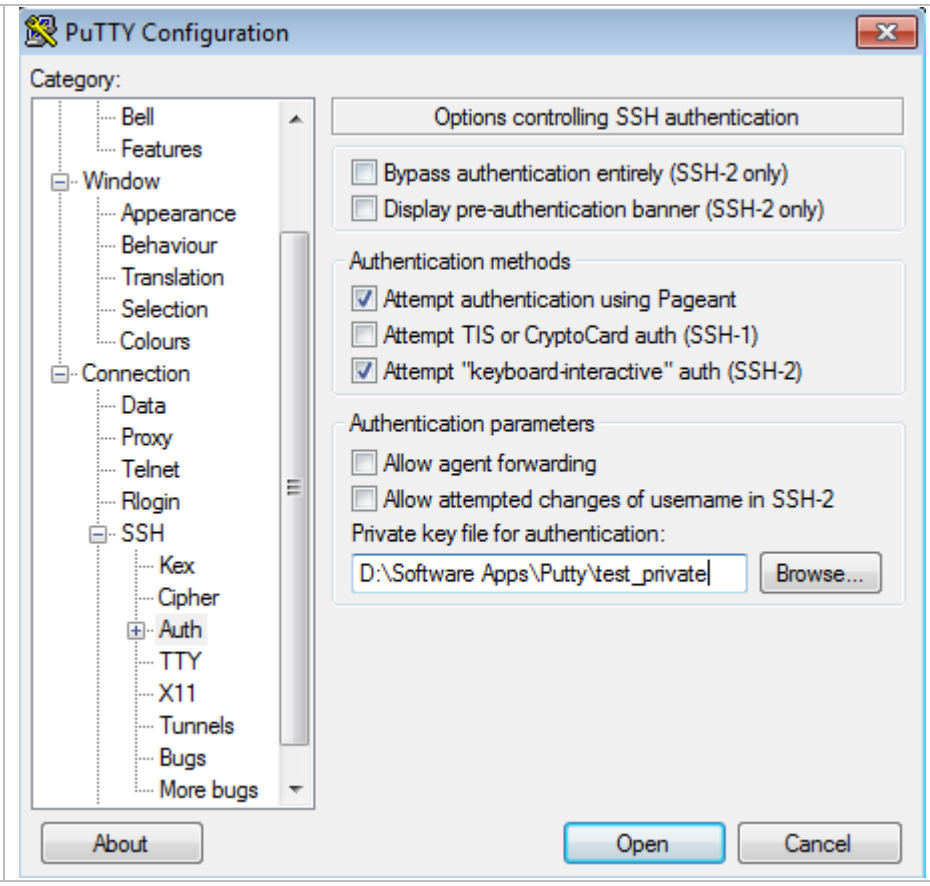


You must select the OpenSSH key file; otherwise, the key file cannot be used. The **puttygen.exe** software can be used to generate a key file in OpenSSH format, but this file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. Format conversion is not required for the public key file stored on the server, and the format of this file is still OpenSSH, as shown in Figure 18-21.

Figure 18-21



SSH Server	Ruijie#configure terminal Ruijie(config)# ip ssh peer test public-key rsaflash:test_key.pub
Verification	● After completing the basic configurations of the client and the server, specify the private key file **test_private** on the PuTTY client, and set the host IP address to **192.168.23.122** and port ID to **22** to set up a connection between the client and the server. In this way, the client can use the public key authentication mode to log in to the network device.
	Figure 18-22



Common Errors

- The **no crypto key generate** command is used to delete a key.

18.4.2 Configuring the SCP Service

Configuration Effect

After the SCP function is enabled on a network device, you can directly download files from the network device and upload local files to the network device. In addition, all interactive data is encrypted, featuring authentication and security.

Notes

- The SSH server must be enabled in advance.

Configuration Steps

Enabling the SCP Server

- Mandatory.
- By default, the SCP server function is disabled. Run the **ip scp server enable** command to enable the SCP server function in global configuration mode.

Configuring the Transmission Path for Files of the SCP Server

- Optional.
- The default transmission path is **flash:/**. Run the **ip scp server topdir {flash:/***path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}** command to configure the transmission path to upload files to or download files from the SCP server.

Verification

Run the **show ip ssh** command to check whether the SCP server function is enabled.

Related Commands

Enabling the SCP Server

Command	**ip scp server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to enable the SCP server. Run the **no ip scp server enable** command to disable the SCP server.

Configuring the Transmission Path for Files of the SCP Server

Command	**ip scp server topdir {flash:/***path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the transmission path to upload files to or download files from the SCP server. Run the **no ip scp server topdir** command to restore the default transmission path.

Configuration Example

Enabling the SCP Server

Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.
	Ruijie#configure terminal Ruijie(config)#ip scp server enable
Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.
	Ruijie(config)#show ipssh

Configuration Steps	● Run the **ip scp server enable** command to enable the SCP server.
	Ruijie#configure terminal Ruijie(config)#ip scp server enable
Verification	● Run the **show ip ssh** command to check whether the SCP server function is enabled.
	Ruijie(config)#show ip ssh SSH Enable - version 1.99 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled

Configuring SSH File Transfer

Scenario **Figure** 18-23	 The SCP service is enabled on the server, and SCP commands are used on the client to transfer data to the server.
Configuration Steps	● Enable the SCP service on the server. The SCP server uses SSH threading. When connecting to a network device for SCP transmission, the client occupies a VTY session (You can finds out that the user type is SSH by running the show user command). ● On the client, use SCP commands to upload files to the server, or download files from the server. Syntax of the SCP command: scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-iidentity_file] [-l limit] [-o ssh_option] [-P port] [-S program] [[user@]host1:]file1 [...] [[user@]host2:]file2 Descriptions of some options: -1: Uses SSHv1 (If not specified, SSHv2 is used by default); -2: Uses SSHv2 (by default);

	-C: Uses compressed transmission. -c: Specifies the encryption algorithm to be used. -r:Transmits the whole directory; -i: Specifies the key file to be used. -l: Limits the transmission speed (unit: Kbit/s). For other parameters, see the filescp.0. Most options are related to terminals. Few options are supported on both terminals and servers. Ruijie's SCP servers do not support d-p-q-r options. When these options are applied, there are prompts.
SSH Server	Ruijie#configure terminal Ruijie(config)# ip scp server enable
Verification	● File transmission example on the Ubuntu 7.10 system: Set the username of a client to **test** and copy the **config.text** file from the network device with the IP address of 192.168.195.188 to the **/root** directory on the local device.
	root@dhcpd:~#scp test@192.168.23.122:/config.text /root/config.text test@192.168.195.188's password: config.text 100% 1506 1.5KB/s 00:00 Read from remote host 192.168.195.188: Connection reset by peer

18.5 Monitoring

Displaying

Description	Command
Displays the effective SSH server configurations.	**show ipssh**
Displays the established SSH connection.	**show ssh**
Displays the public information of the SSH public key.	**show crypto key mypubkey**

Debugging

⚠ System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SSH sessions.	**debug ssh**

19 Configuring GSN

19.1 Overview

Global Security Network (GSN) is a security policy platform consisting of a series of security policies such as access control and network security. The GSN platform includes a device end and a server end. RG Security Policy Management Platform (RG-SMP) server acts as the security policy server for GSN.

In Ruijie General Operation System (RGOS), GSN accepts policies assigned by the SMP server, installs the policies on devices, and determines whether to allow data packets in a certain condition to pass through RG Security Switch. The security policies include binding, isolation, and blocking. Binding is to bind the IP address and MAC address of a user (usually authenticated by the server) on a device. Isolation and blocking are to allow or prohibit transmission of specific data by setting an Access Control List (ACL).

GSN collaborates with the SMP server, 802.1X authentication, and Web authentication.

19.2 Applications

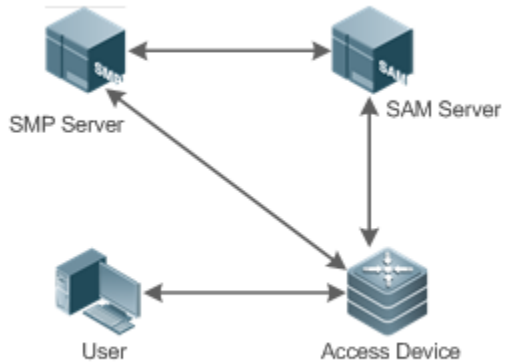
Application	Description
GSN Security Protection for Authenticated Users	After a user passes 802.1X authentication, the SMP server assigns security policies (such as ARP guard and device integrity) to maintain the user's network security.

19.2.1 GSN Security Protection for Authenticated Users

Scenario

After a user passes 802.1X authentication, the SMP server learns the IP-MAC mapping of this user from the Security Account Manager (SAM) server and then assigns security policies to the access device.

Figure 19-1



Remarks	Process description: 1. The user passes 802.1X authentication. 2. The SAM server reports user information to the SMP server. 3. After successful authentication, the access device determines whether to adopt the address binding policy for the user based on the configuration. 4. The user exchanges packets with the SMP server in real time, and the access device converts the packet format and forwards the packets. 5. The SMP server assigns security policies to the access device based on information reported by the user. 6. Besides, the SMP server periodically or manually synchronizes policies with the switch. If the SMP server finds that the policies maintained on itself are different from those maintained on the access switch, it deletes all policies on the access device, and then installs all policies maintained on itself onto the access device. 7. During steps 3, 5, and 6, the access device synchronizes and installs the policies based on the policies of GSN.

Deployment

- Enable 802.1X authentication on the access device and deploy the SAM server.
- Deploy the SMP server and add the access device to receive security policies assigned.
- Enable GSN and address binding on the access device.

19.3 Features

Basic Concepts

↘ Ruijie Security Solution

Ruijie security solution is composed of the following four elements:

- RG-SMP platform
- RG Security Agent
- RG Restore System
- RG Security Switch

↘ RG-SMP Platform

Based on the configured policies, the RG-SMP platform determines whether to allow data packets specified in a certain range to pass through RG Security Switch. To install policies is to set policies on a device. To uninstall policies is to remove policies from a device.

RG Security Agent

RG Security Agent is a type of software running on each device that has accessed a corporate network. It collects device information, identifies users' network behaviors, monitors network communication and security status of the devices, and sends collected information to the RG-SMP platform so that the administrator can make security policies accordingly. RG Security Agent automatically downloads new security policies from the RG-SMP platform and implements specified security policies locally.

RG Restore System

If abnormal behaviors occur, RG Restore System works as follows:

For users failing to meet corporate security policies, the administrator presets policies on the RG-SMP platform to shield most of the network access permissions of these unauthorized users and leave only one green security channel. This security channel can only connect to corporate security policy upgrade servers, including the Windows patch upgrade server, virus upgrade library server for anti-virus software, or other corporate upgrade servers.

When detecting that the security policies of a device do not meet the security levels defined by the RG-SMP platform, RG Security Agent immediately uploads its security logs to the RG-SMP platform. The RG-SMP platform selects one policy from the preset policy set based on the alarm logs sent by RG Security Agent, and sends this policy to all RG security switches. After accepting the latest policy configuration, RG security switches immediately apply the configuration so that the alarming user can access only the specified upgrade server based on the restoration operations specified by the SMP server and automatically install patches.

When the user completes all restoration operations specified by the SMP server, RG Security Agent checks the security of the RG-SMP platform again. If the user meets all security policy sets, RG Security Agent notifies the RG-SMP platform to cancel the ACL restriction on this user and set this user to a common user.

RG Security Switch

As a part of Ruijie security solution, RG Security Switch receives policies from the RG-SMP platform, installs the policies, and controls users based on the installed policies.

19.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to enable GSN on an access device and its communication with the SMP server.	
	security gsn enable	Globally enables GSN. GSN is disabled by default.
	security { [**v1** | **v2**] **community** *community* | **v3 user** *username* }	Configures the name of the security authentication mechanism used for communication with the SMP server.

	smp-server host *ip-address*	Configures the IP address of the SMP server.
	(Optional) It is used to configure the minimum interval for transmitting security events.	
	security event interval *interval*	Configures the minimum interval for transmitting security events. The **interval** value ranges from 1 to 65,535 seconds. The default value is 5 seconds.
Enabling WLAN-based Address Binding	(Optional) It is used to enable address binding on a Wireless Local Area Network (WLAN).	
	gsn address-bind	Enables WLAN-based address binding. This policy is disabled by default.

19.4.1 Configuring GSN Basic Functions

Configuration Effect

- Globally enable GSN on devices.
- Enable devices to communicate with the SMP server.

Notes

- You can configure SNMPv1, SNMPv2, or SNMPv3 as the name of the security authentication mechanism for communication with the SMP server.
- To facilitate user configuration, **security v1 community** and **security community** are both used to configure SNMPv1. If SNMPv3 is selected, you must configure SNMPv3 users under the **snmp-server** command. For details about configuration commands, refer to the section *Configuring SNMP*.
- Do not exceed the number of entries supported by GSN.

Configuration Steps

Globally Enabling GSN

- Mandatory.
- Unless otherwise specified, enable GSN on each device that requires the security solution.

Enabling Communication with the SMP Server

- Mandatory.
- Unless otherwise specified, enable this function on each device that requires the security solution to communicate with the SMP server.

Configuring the IP Address of the SMP Server

- Mandatory.
- Unless otherwise specified, configure the IP address of the SMP server on each device that requires the security solution to communicate with the SMP server.

Configuring the Minimum Interval for Transmitting Security Events

- To prevent unauthorized users from frequently sending security events to attack RG Security Switch and the SMP server by faking security events, you can configure the minimum interval for transmitting security events to restrict users from reporting security events.
- If you want to modify the default minimum interval for transmitting the security events, run the related command. The default interval is 5 seconds.

Related Commands

Globally Enabling GSN

Command	**security gsn enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Communication with the SMP Server

Command	**security** { [**v1** | **v2**] **community** *community* | **v3 user** *username* }
Parameter Description	**community** *community*: Specifies the name of the security authentication mechanism for communication with the SMP server. **user** *username*: Indicates the name of an SNMPv3 user.
Command Mode	Global configuration mode
Usage Guide	To facilitate user configuration, **security v1 community** and **security community** are both used to configure SNMPv1. If SNMPv3 is selected, you must configure SNMPv3 users under the **snmp-server** command. For details about configuration commands, refer to the section *Configuring SNMP*.

Configuring the IP Address of the SMP Server

Command	**smp-server host** *ip-address*
Parameter Description	*ip-address*: Specifies the IP address of the SMP server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Minimum Interval for Transmitting Security Events

Command	**security event interval** *interval*
Parameter Description	**interval** *interval*: Specifies the minimum interval for transmitting security events. The value ranges from 1 to 65,535 seconds. The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling GSN and the Communication with the SMP Server

Configuration Steps	● Globally enable GSN on the device. ● Configure the name of the security authentication mechanism for devices to communicate with the SMP server. ● Configure the IP address of the SMP server.
	Ruijie# configure terminal Ruijie(config)# security gsn enable Ruijie(config)# security v1 community test-name Ruijie(config)# smp-server host 192.168.30.9 Ruijie(config)# exit
Verification	Run the following **show** commands: ● Run the **show smp-server** command to display the IP address of the SMP server. ● Run the **show security event interval** command to display the minimum interval for transmitting security events.
	Ruijie# show smp-server SMP-Server IP:192.168.30.9 Ruijie# show security event interval Event sending interval(Seconds):5

Common Errors

- Routes to the SMP server are unavailable.

19.4.2 Enabling WLAN-based Address Binding

Configuration Effect

- Enable address binding on a WLAN.

Notes

This function takes effect only when GSN is globally enabled and the WLAN security mode is set to Wi-Fi Protected Access (WPA) or WPA2.

Due to the application features of GSN, you need to disable 802.1X-based IP address authorization before enabling GSN. GSN and 802.1X-based IP address authorization cannot be enabled at the same time. Otherwise, the running of security policies will be affected.

Configuration Steps

Enabling WLAN-based Address Binding

- To enable address binding based on a WLAN, run the **gsn address-bind** command.

Related Commands

Enabling WLAN-based Address Binding

Command	**gsn address-bind**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Enabling WLAN-based Address Binding

Configuration Steps	• Create a WLAN. • Enter the WLAN security configuration mode. • Enable WLAN-based address binding.
	Ruijie# configure terminal Ruijie(config)# wlansec 100 Ruijie(config-wlansec)# gsn address-bind Ruijie(config)# exit

19.5 Monitoring

Displaying

Description	Command
Displays the IP address of the SMP server.	**show smp-server**
Displays the minimum interval for transmitting security events.	**show security event interval**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs GSN.	**debug gsn** { **all** | **error** | **event** | **packet** | **server** | **detail** }

20 Configuring SUMNG

20.1 Overview

Security User Manage (SUMNG) is a component for the AC/AP to manage security account information, providing valid identity authentication for wireless access. It mainly provides the identity authentication and client management services for Personal Pre-Shared Key (PPSK) authentication.

With PPSK authentication, each client has an independent key. Compared with the traditional PSK authentication that shares one key by all clients, PPSK features high security, easy deployment, and low cost.

SUMNG mainly implements user management and PPSK authentication by providing client-based passwords for PSK authentication:

1. User management
2. PPSK authentication

Protocols and Standards

- N/A

20.2 Applications

Application	Description
PPSK Authentication Network	Small and medium enterprises with less than 500 employees do not have background servers deployed, and impose high requirements on wireless network security.

20.2.1 PPSK Authentication Network

Scenario

SUMNG provides the PPSK authentication network with client-based PSK keys, to implement PPSK authentication on clients with different PSK keys.

Deployment

- Configure an office network SSID on the AC to enable PPSK authentication.

20.3 Features

Basic Concepts

↘ **WiFi Key Pool**

- SUMNG generates an independent WiFi key based on the user identity, and provides it for only one client.
- SUMNG can generate a maximum of 1500 keys. Multiple keys can be generated for each user name, but the total number of keys cannot exceed the upper limit (1500).
- PPSK authentication can be enabled in only one WLAN.

Overview

Feature	Description
User Management	Generates and manages WiFi keys of users.
PPSK Authentication	Implements PPSK authentication based on the independent WiFi key of each client.

20.3.1 User Management

Manage WiFi keys of users, including the user identities.

Working Principle

The administrator adds a user identity (user name or email or the like) on the AC to generate a WiFi key. The WiFi key is stored on the device and remains unchanged during process restart and device restart. After the client uses the WiFi key to connect to the network, the MAC address, WiFi key, and user identity are bound together.

20.3.2 PPSK Authentication

Use the registered client data to implement higher-security PPSK authentication on clients with different passwords.

Working Principle

When connecting to a PPSK signal, a client obtains the corresponding key from the SUMNG client database based on the MAC address. If the client finds the corresponding key (the client is successfully registered), it uses the key to perform 4-way handshake authentication. If the client fails to find the corresponding key, it is an invalid client and cannot access the network.

20.4 Configuration

Configuration	Description and Command	
Basic SUMNG Configurations	⚠ (Mandatory) It is used to enable PPSK authentication and generate a WiFi key.	
	security sta-psk enable	Enables PPSK authentication.
	sumng username	Generates a WiFi key.
Optional SUMNG Configurations	⚠ Optional.	
	sumng log enable	Configures the output of syslogs.
	sumng log rate-limit	Configures the rate limit of outputting syslogs.

20.4.1 Basic SUMNG Configurations

Configuration Effect

- Enter a user identity to generate a WiFi key, to provide services for PPSK authentication.

Notes

- Because the number of WiFi keys is limited, do not waste the generated WiFi keys.

Configuration Steps

↘ Enabling PPSK Authentication

- Mandatory.
- PPSK must be enabled.

Command	**security sta-psk enable**
Parameter Description	N/A
Defaults	PPSK is not enabled by default.
Command Mode	WLANSec configuration mode
Usage Guide	`This command should be used together with the` **`security rsn enable, security rsn akm psk enable, and security rsn ciphers aes enable`** `commands.`

Verification

- Run the **show running** command to display the configurations.

↘ Configuring a Security User Account

- Mandatory.
- Generate a WiFi key first, so that the client can connect to the network using the WiFi key.

Command	**sumng username** *uname*
Parameter Description	*uname*: Indicates the user identity.
Defaults	No security user account is configured by default.
Command Mode	Global configuration mode
Usage Guide	A WiFi key is generated upon user application. The user name is not unique for generating keys. That is, two keys are generated if a user name is used twice.

Verification

- Run the **show sumng user name** command to display the configurations.

Command	**show sumng user name** *uname*
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	This command is used to display the generated WiFi key.
Command Presentation	Ruijie#show sumng user name test UserName WifiKey Account-Time Mac-Address Reg-Time ---------- ---------- ---------- ---------- ---------- test 23Q92w3AzMUJJ Tue Feb 7 15:49:20 2017 a03b.e38e.0565 Wed Feb 8 19:43:53 2017 Ruijie#

20.4.2 Optional SUMNG Configurations

Configuration Effect

- Use optional configurations to meet different scenario requirements.

Notes

Configuration Steps

Configuring the Output of Syslogs

- Optional.
- Syslogs are output by default when the SUMNG client is bound. You can disable the output of syslogs.

Command	**sumng log enable**
Parameter Description	N/A
Defaults	The output of syslogs is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rate Limit of Outputting Syslogs

- Optional.
- The output of syslogs consumes device resources. Limit the syslog output to prevent impact on the normal service operation.

Command	**sumng log rate-limit** *num*
Parameter Description	*num*: Indicates the number of syslogs output per second.
Defaults	A maximum of 5 syslogs are output per second by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to display the configurations.

Configuration Example

Enabling PPSK Authentication

Configuration Steps	• Enable PPSK authentication.
	`Ruijie(config)#wlansec 1` `Ruijie(config-wlansec)#security rsn enable` `Ruijie(config-wlansec)#security rsn akm psk enable` `Ruijie(config-wlansec)#security rsn ciphers aes enable` `Ruijie(config-wlansec)#security sta-psk enable`

Generating a WiFi Key

Configuration Steps	• Generate a WiFi key.
	`Ruijie(config)#sumng username test` `Ruijie(config)#show sumng user name test` `UserName WifiKey Account-Time Mac-Address Reg-Time` `---------- ---------- ---------- ---------- ----------` `test 23Q92w3AzMUJJ Tue Feb 7 15:49:20 2017 a03b.e38e.0565 Wed Feb 8 19:43:53 2017` `Ruijie#`

20.5 Monitoring

Displaying

Description	Command
Displays SUMNG user information.	**show sumng user {all | name** *name-string***}**

Debugging

System resources are occupied when debugging information is output. Therefore, disable the debugging switch immediately after use.

Description	Command
Debugs the SUMNG event.	**debug sumng event**
Debugs the SUMNG details.	**debug sumng detail**
Debugs the SUMNG error.	**debug sumng error**
Debugs the SUMNG key information.	**debug sumng info**

System Configuration

1. Configuring CLI
2. Configuring Basic Management
3. Configuring Lines
4. Configuring RMON
5. Configuring SNMP
6. Configuring HTTP Service
7. Configuring Syslog
8. Configuring CWMP
9. Configuring LED
10. Configuring Software Authorization Management
11. Configuring USB
12. Configuring PKG_MGMT

13. Configuring NTP
14. Configuring SNTP
15. Configuring SPAN-RSPAN
16. Configuring Time Range

1 Configuring CLI

1.1 Overview

The command line interface (CLI) is a window used for text command interaction between users and network devices. You can enter commands in the CLI window to configure and manage network devices.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Configuring and Managing Network Devices Through CLI	You can enter commands in the CLI window to configure and manage network devices

1.2.1 Configuring and Managing Network Devices Through CLI

Scenario

As shown in Figure 1-1, a user accesses network device A using a PC, and enter commands in the CLI window to configure and manage the network device.

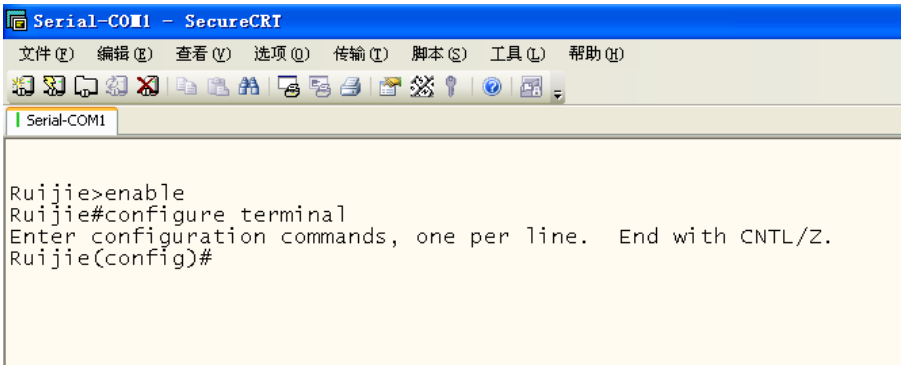
Figure 1-1

Remarks	A is the network device to be managed. PC is a terminal.

Deployment

As shown in Figure 1-2, the user uses the Secure CRT installed on a PC to set up a connection with network device A, and opens the CLI window to enter configuration commands.

Figure 1-2



1.3 Features

Overview

Feature	Description
Accessing CLI	You can log in to a network device for configuration and management.
Command Modes	The CLI provides several command modes. Commands that can be used vary according to command modes.
System Help	You can obtain the help information of the system during CLI configuration.
Abbreviated Commands	If the entered string is sufficient to identify a unique command, you do not need to enter the full string of the command.
No and Default Options of Commands	You can use the **no** option of a command to disable a function or perform the operation opposite to the command, or use the **default** option of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error prompt will be displayed if an incorrect command is entered.
History Commands	You can use short-cut keys to display or call history commands.
Featured Editing	The system provides short-cut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the **show** command to search or filter specified commands.
Command Alias	You can configure alias of a command to replace the command.

1.3.1 Accessing CLI

Before using the CLI, you need to connect a terminal or PC to a network device. You can use the CLI after starting the network device and finishing hardware and software initialization. When used for the first time, the network device can be connected only through the console port, which is called out band management. After performing relevant configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

Due to the large number of commands, these commands are classified by function to facilitate the use of commands. The CLI provides several commands modes, and all commands are registered in one or several command modes. You must first enter the command mode of a command before using this command. Different command modes are related with each other while distinguished from each other.

As soon as a new session is set up with the network device management interface, you enter User EXEC mode. In this mode, you can use only a small number of commands and the command functions are limited, such as the **show** commands. Execution results of commands in User EXEC mode are not saved.

To use more commands, you must first enter Privileged EXEC mode. Generally, you must enter a password to enter Privileged EXEC mode. In Privileged EXEC mode, you can use all commands registered in this command mode, and further enter global configuration mode.

Using commands of a certain configuration mode (such as global configuration mode and interface configuration mode) will affect configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter global configuration mode before entering another configuration mode, such as interface configuration mode.

The following table summarizes the command modes by assuming that the name of the network device is “Ruijie”.

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
User EXEC (User EXEC mode)	Enter User EXEC mode by default when accessing a network device.	Ruijie>	Run the **exit** command to exit User EXEC mode. Run the **enable** command to enter Privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC (Privileged EXEC mode)	In User EXEC mode, run the **enable** command to enter Privileged EXEC mode.	Ruijie#	Run the **disable** command to return to User EXEC mode. Run the **configure** command to enter global configuration mode.	Use this command mode to check whether the configuration takes effect. This mode is password protected.

Command Mode	Access Method	Prompt	Exit or Entering Another Mode	About
Global configuration (Global configuration mode)	In Privileged EXEC mode, run the **configure** command to enter global configuration mode.	Ruijie(config)#	Run the **exit** or **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **interface** command to enter interface configuration mode. When using the **interface** command, you must specify the interface. Run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Using commands in this mode will affect the global parameters of the network device.
Interface configuration (Interface configuration mode)	In global configuration mode, run the **interface** command to enter interface configuration mode.	Ruijie(config-if)#	Run the **end** command, or press **Ctrl+C** to return to Privileged EXEC mode. Run the **exit** command to return to global configuration mode. When using the **interface** command, you must specify the interface.	Use this configuration mode to configure various interfaces of the network device.
Config-vlan (VLAN configuration mode)	In global configuration mode, run the **vlan** *vlan_id* command to enter VLAN configuration mode.	Ruijie(config-vlan)#	Run the **end** command, or press **Ctrl+C** to return to the Privileged EXEC mode. Run the **exit** command to return to global configuration mode.	Use this configuration mode to configure VLAN parameters.

1.3.3 System Help

When entering commands in the CLI window, you can obtain the help information using the following methods:

1. At the command prompt in any mode, enter a question mark (?) to list the commands supported by the current command mode and related command description.

For example

```
Ruijie>?

Exec commands:

  <1-99>      Session number to resume
```

```
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  help        Description of the interactive help system
  lock        Lock the terminal
  ping        Send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

2. Enter a space and a question mark (?) after a keyword of a command to list the next keyword or variable associated with the keyword.

For example

```
Ruijie(config)#interface ?
  Aggregateport     Aggregate port interface
  Dialer            Dialer interface
  GigabitEthernet   Gigabit Ethernet interface
  Loopback          Loopback interface
  Multilink         Multilink-group  interface
  Null              Null interface
  Tunnel            Tunnel interface
  Virtual-ppp       Virtual PPP interface
  Virtual-template  Virtual Template interface
  Vlan              Vlan interface
  range             Interface range command
```

If the keyword is followed by a parameter value, the value range and description of this parameter are displayed as follows:

```
Ruijie(config)#interface vlan ?
  <1-4094>  Vlan port number
```

3. Enter a question mark (?) after an incomplete string of a command keyword to list all command keywords starting with the string.

For example

```
Ruijie#d?
debug  delete  diagnostic  dir  disable  disconnect
```

4. After an incomplete command keyword is entered, if the suffix of this keyword is unique, press the **Tab** key to display the complete keyword.

For example

```
Ruijie# show conf<Tab>
Ruijie# show configuration
```

5. In any command mode, run the **help** command to obtain brief description about the help system.

For example

```
Ruijie(config)#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

1.3.4 Abbreviated Commands

If a command is long, you can enter a part of the command that is sufficient to identify the command keyword.

For example, to run the **interface** *gigabitEthernet 0/1* command in GigabitEthernet 0/1 interface configuration mode, enter the abbreviated command as follows:

```
Ruijie(config)#int g0/1
Ruijie(config-if-GigabitEthernet 0/1)#
```

1.3.5 No and Default Options of Commands

Most commands have the **no** option. Generally, the **no** option is used to disable a feature or function, or perform the operation opposite to the command. For example, run the **no shutdown** command to perform the operation opposite to the **shutdown** command, that is, enabling the interface. The keyword without the **no** option is used to enable a disabled feature or a feature that is disabled by default.

Most configuration commands have the **default** option. The **default** option is used to restore default settings of the command. Default values of most commands are used to disable related functions. Therefore, the function of the **default** option is the same as that of the **no** option in most cases. For some commands, however, the default values are used to enable related functions. In this case, the function of the **default** option is opposite to that of the **no** option. At this time, the **default** option is used to enable the related function and set the variables to default values.

For specific function of the **no** or **default** option of each command, see the command reference.

1.3.6 Prompts Indicating Incorrect Commands

When you enter an incorrect command, an error prompt is displayed.

The following table lists the common CLI error messages.

Error Message	Meaning	How to Obtain Help
% Ambiguous command: "show c"	The characters entered are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark after the word that is ambiguous. All the possible keywords will be displayed.
% Incomplete command.	The mandatory keyword or variable is not entered in the command.	Re-enter the command, and enter a space and a question mark. All the possible keywords or variables will be displayed.
% Invalid input detected at '^' marker.	An incorrect command is entered. The sign (^) indicates the position of the word that causes the error.	At the current command mode prompt, enter a question mark. All the command keywords allowed in this command mode will be displayed.

1.3.7 History Commands

The system automatically saves commands that are entered recently. You can use short-cut keys to display or call history commands.

The methods are described in the following table.

Operation	Result
Ctrl+P or the UP key	Display the previous command in the history command list. Starting from the latest record, you can repeatedly perform this operation to query earlier records.
Ctrl+N or the DOWN key	After pressing Ctrl+N or the DOWN key, you can return to a command that is recently executed in the history command list. You can repeatedly perform this operation to query recently executed commands.

The standard terminals, such as the VT100 series, support the direction keys.

1.3.8 Featured Editing

When editing the command line, you can use the keys or short-cut keys listed in the following table:

Function	Key or Short-Cut Key	Description
Move the cursor on the	Left key or Ctrl+B	Move the cursor to the previous character.

Function	Key or Short-Cut Key	Description
editing line.	Right key or Ctrl+F	Move the cursor to the next character.
	Ctrl+A	Move the cursor to the head of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete an entered character.	Backspace key	Delete one character to the left of the cursor.
	Delete key	Delete one character to the right of the cursor.
Move the output by one line or one page.	Return key	When displaying contents, press the **Return** key to move the output one line upward and display the next line. This operation is performed when the output does not end yet.
	Space key	When displaying contents, press the **Space** key to page down and display the next page. This operation is performed when the output does not end yet.

When the editing cursor is close to the right boundary, the entire command line will move to the left by 20 characters, and the hidden front part is replaced by the dollar ($) signs. You can use the related keys or short-cut keys to move the cursor to the characters in the front or return to the head of the command line.

For example, the whole **access-list** may exceed the screen width. When the cursor is close to the end of the command line for the first time, the entire command line moves to the left by 20 characters, and the hidden front part is replaced by the dollar signs ($). Each time the cursor is close to the right boundary, the entire command line moves to the left by 20 characters.

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
$0.220 host 202.101.99.12 time-range tr
```

Press **Ctrl+A** to return to the head of the command line. At this time, the hidden tail part of the command line is replaced by the dollar signs ($).

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

The default screen width is 80 characters.

1.3.9 Searching and Filtering of the Show Command Output

To search specified contents from the output of the **show** command, run the following command:

Command	Description
show *any-command* | **begin** *regular-expression*	Searches specified contents from the output of the **show** command. The first line containing the contents and all information that follows this line will be output.

The **show** command can be executed in any mode.

Searched contents are case sensitive.

To filter specified contents from the output of the **show** command, run the following commands:

Command	Description
show *any-command* | **exclude** *regular-expression*	Filters the output of the **show** command. Except those containing the specified contents, all lines will be output.
show *any-command* | **include** *regular-expression*	Filters the output of the **show** command. Only the lines containing the specified contents will be output.

To search or filter the output of the **show** command, you must enter a vertical line (|). After the vertical line, select the searching or filtering rules and contents (character or string). Searched and filtered contents are case sensitive.

```
Ruijie#show running-config | include interface

interface GigabitEthernet 0/0

interface GigabitEthernet 0/1

interface GigabitEthernet 0/2

interface GigabitEthernet 0/3

interface GigabitEthernet 0/4

interface GigabitEthernet 0/5

interface GigabitEthernet 0/6

interface GigabitEthernet 0/7

interface Mgmt 0
```

1.3.10 Command Alias

You can configure any word as the alias of a command to simply the command input.

Configuration Effect

1. Replace a command with a word.

For example, configure "mygateway" as the alias of the **ip route** *0.0.0.0 0.0.0.0192.1.1.1* command. To run this command, you only need to enter "mygateway".

2. Replace the front part of a command with a word, and enter the later part.

For example, configure "ia" as the alias of the **ip address** command. To run this command, you need to enter "ia" and then the specified IP address and subnet mask.

Configuration Steps

↘ Displaying Default Alias

In User EXEC or Privileged EXEC mode, default alias are available for some commands. You can run the **show aliases** command to display these default aliases.

```
Ruijie(config)#show aliases

Exec mode alias:
```

```
h                   help
p                   ping
s                   show
u                   undebug
un                  undebug
```

These default aliases cannot be deleted.

Configuring a Command Alias

Command	**alias** *mode command-alias original-command*
Parameter Description	*mode*: indicates the command mode of the command represented by the alias. *command-alias*: indicates the command alias. *original-command*: indicates the command represented by the alias.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, run the **alias** ? command to list all command modes that can be configured with aliases.

Displaying Settings of Command Aliases

Run the **show aliases** command to display alias settings in the system.

Notes

- The command replaced by an alias must start from the first character of the command line.
- The command replaced by an alias must be complete.
- The entire alias must be entered when the alias is used; otherwise, the alias cannot be identified.

Configuration Example

Defining an Alias to Replace the Entire Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the default route configuration command **ip route** *0.0.0.0 0.0.0.0 192.168.1.1.*
	`Ruijie#configure terminal` `Ruijie(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1`
Verification	● Run the **show alias** command to check whether the alias is configured successfully. `Ruijie(config)#show alias` `Exec mode alias:` `  h  help` `  p  ping`

	s show u undebug un undebug Global configuration mode alias: ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
	● Use the configured alias to run the command, and run the **show running-config** command to check whether the alias is configured successfully.
	Ruijie(config)#ir Ruijie(config)#show running-config Building configuration... ! alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuring an alias ... ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" is entered !

Defining an Alias to Replace the Front Part of a Command

Configuration Steps	In global configuration mode, configure the alias "ir" to represent the front part "**ip route**" of the default route configuration command.
	Ruijie#configure terminal Ruijie(config)#alias config ir ip route
Verification	● Run the **show alias** command to check whether the alias is configured successfully. Ruijie(config)#show alias Exec mode alias: h help p ping s show u undebug un undebug Global configuration mode alias: ir ip route
	● Enter the alias "ir" and then the later part of the command "0.0.0.0 0.0.0.0 192.168.1.1".

	● Run the **show ap-config running** command to check whether the configuration is successful.
	Ruijie(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1 Ruijie(config)#show running Building configuration... ! alias config ir ip route //Configuring an alias ! ip route 0.0.0.0 0.0.0.0 192.168.1.1 //Configuration result after the alias "ir" and the later part of the command are entered !

System Help

1. The system provides help information for command alias. An asterisk (*) will be displayed in front of an alias. The format is as follows:

```
*command-alias=original-command
```

For example, in Privileged EXEC mode, the default command alias "s" represents the **show** keyword. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
Ruijie#s?
*s=show  show  start-chat  start-terminal-service
```

2. If the command represented by an alias contains more than one word, the command is displayed in a pair of quotation marks.

For example, in Privileged EXEC mode, configure the alias "sv" to replace the **show version** command. If you enter "s?", the keywords starting by "s" and alias information are displayed.

```
Ruijie#s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

3. You can use the alias to obtain help information about the command represented by the alias.

For example, configure the alias "ia" to represent the **ip address** command in interface configuration mode. If you enter "ia?" in interface configuration mode, the help information on "ip address?" is displayed, and the alias is replaced by the command.

```
Ruijie(config-if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
```

```
Ruijie(config-if)#ip address
```

If you enter a space in front of a command, the command represented by this alias will not be displayed.

2 Configuring Basic Management

2.1 Overview

This document is a getting started guide to network device management. It describes how to manage, monitor, and maintain network devices.

2.2 Applications

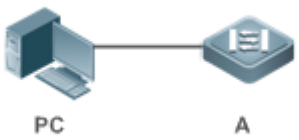
Application	Description
Network Device Management	A user logs in to a network device from a terminal and runs commands on a command line interface (CLI) to manage device configurations.

2.2.1 Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to Network Device A from a terminal and runs commands on the CLI to manage device configurations. See Figure 2-1.

Figure 2-1



2.3 Features

Basic Concepts

↘ TFTP

Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol which allows a client to transfer a file to a server or get a file from a server.

↘ AAA

AAA is short for Authentication, Authorization and Accounting.

Authentication refers to the verification of user identities and the related network services.

Authorization refers to the granting of network services to users according to authentication results.

Accounting refers to the tracking of network service consumption by users. A billing system charges users based on consumption records.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is the most widely used AAA protocol at present.

Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol stack which provides access to a remote host through a virtual terminal connection. It is a standard protocol located at Layer 7 (application layer) of the Open System Interconnection (OSI) model and used on the internet for remote login. Telnet sets up a connection between the local PC and a remote host.

System Information

System information includes the system description, power-on time, hardware and software versions, control-layer software version, and boot-layer software version.

Hardware Information

Hardware information includes the physical device information as well as slot and module information. The device information includes the device description and slot quantity. The slot information includes the slot ID, module description (which is empty if a slot does not have a module), and actual and maximum number of physical ports.

Overview

Feature	Description
User Access Control	Controls the terminal access to network devices on the internet based on passwords and privileges.
Login Authentication Control	Performs username-password authentication to grant access to network devices when AAA is enabled. (Authentication is performed by a dedicated server.)
Basic System Parameters	Refer to the parameters of a system, such as the clock, banner, and Console baud rate.
Displaying Configurations	Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the nonvolatile random access memory (NVRAM).
Telnet	Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.
Restart	Introduces system restart.

2.3.1 User Access Control

User access control refers to the control of terminal access to network devices on the internet based on passwords and privileges.

Working Principle

Privilege Level

16 privilege levels are defined ranging from 0 to 15 for CLI on network devices to grant users access to different commands. Level 0 is the lowest level granting access to just a few commands, whereas level 15 is the highest level granting access to all commands. Levels 0 and 1 are common user levels without the device configuration permission (users are not allowed to enter global configuration mode by default). Levels 2–15 are privileged user levels with the device configuration permission.

Password Classification

Passwords are classified into two types: password and security. The first type refers to simple encrypted passwords at level 15. The second type refers to secure encrypted passwords at levels 0–15. If a level is configured with both simple and secure encrypted passwords, the simple encrypted password will not take effect. If you configure a non-15 level simple encrypted password, a warning is displayed and the password is automatically converted into a secure encrypted password. If you configure the same simple encrypted password and secure encrypted password at level 15, a warning is displayed.

Password Protection

Each privilege level on a network device has a password. An increase in privilege level requires the input of the target level password, whereas a reduction in privilege level does not require password input.

By default, only two privilege levels are password-protected, namely, level 1 (common user level) and level 15 (privileged user level). Sixteen privilege levels with password protection can be assigned to the commands in each mode to grant access to different commands.

If no password is configured for a privileged user level, access to this level does not require password input. It is recommended that a password be configured for security purposes.

Command Authorization

Each command has its lowest execution level. A user with a privilege level lower than this level is not allowed to run the command. After the command is assigned a privilege level, users at this level and higher have access to the command.

Related Configuration

Configuring a Simple Encrypted Password

- Run the **enable password** command.

Configuring a Secure Encrypted Password

- Run the **enable secret** command.
- A secure encrypted password is used to control the switching between user levels. It has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

Configuring Command Privilege Levels

- Run the **privilege** command to assign a privilege level to a command.
- A command at a lower level is accessible by more users than a command at a higher level.

Raising/Lowering a User Privilege Level

- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.
- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.

Enabling Line Password Protection

- Line password protection is required for remote login (such as login through Telnet).
- Run the **password**[**0** | **7**] *line* command to configure a line password, and then run the **login** command to enable password protection.
- By default, terminals do not support the **lock** command.

2.3.2 Login Authentication Control

In login authentication with AAA disabled, the password entered by a user is checked against the configured line password. If they are consistent, the user can access the network device. In local authentication, the username and password entered by a user are checked against those stored in the local user database. If they are matched, the user can access the network device with proper management permissions.

In AAA, the username and password entered by a user are authenticated by a server. If authentication is successful, the user can access the network device and enjoy certain management permissions.

For example, a RADIUS server can be used to authenticate usernames and passwords and control users' management permissions on network devices. Network devices no longer store users' passwords, but send encrypted user information to the RADIUS server, including usernames, passwords, shared passwords, and access policies. This provides a convenient way to manage and control user access and improve user information security.

Working Principle

Line Password

If AAA is disabled, you can configure a line password used to verify user identities during login. After AAA is enabled, line password verification does not take effect.

Local Authentication

If AAA is disabled, you can configure local authentication to verify user identities and control management permissions by using the local user database. After AAA is enabled, local authentication does not take effect.

AAA

AAA provides three independent security functions, namely, Authentication, Authorization and Accounting. A server (or the local user database) is used to perform authentication based on the configured login authentication method list and control users' management permissions. For details about AAA, see *Configuring AAA*.

Related Configuration

Configuring Local User Information

- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.

Configuring Local Authentication for Line-Based Login

- Run the **login local** command (in the case that AAA is disabled).
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- The default authentication method is used after AAA is enabled.
- Run the **login authentication** command to configure a login authentication method list for a line.
- Perform this configuration when the local AAA authentication is required.

Configuring the Connection Timeout Time

- The default connection timeout time is 10 minutes.
- Run the **exec-timeout** command to change the default connection timeout time. An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- The default session timeout time is 0 minutes, indicating no timeout.
- Run the **session-timeout** command to change the default session timeout time.
- The session established to a remote host through a line will be disconnected if no output is detected during the timeout time. Then the remote host is restored to Idle. Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- By default, terminals do not support the **lock** command.
- Run the **lockable** command to lock the terminals connected to the current line.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command in terminal EXEC mode to lock the terminal.

2.3.3 Basic System Parameters

System Time

The network device system clock records the time of events on the device. For example, the time shown in system logs is obtained from the system clock. Time is recorded in the format of *year-month-day, hour*:*minute*:*second*, *day of the week*.

When you use a network device for the first time, set its system clock to the current date and time manually.

Configuring a System Name and Command Prompt

You can configure a system name to identify a network device. The default system name is **Ruijie**. A name with more than 32 characters will be truncated to keep only the first 32 characters. The command prompt keeps consistent with the system name.

Banner

A banner is used to display login prompt information. There are two types of banner: Daily notification and login banner.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.
- A login banner appears after daily notification to display login information.

Configuring the Console Baud Rate

You can manage network device through a Console port The first configuration on the network device must be performed through the Console port. The serial port baud rate can be changed based on actual requirements. Note that the management terminal must have consistent baud rate setting with the device console.

Configuring the Connection Timeout Time

The connection timeout time is used to control device connections (including established connections and sessions established to remote hosts). A connection will be closed when no input is detected during the timeout time.

Related Configuration

Configuring the System Date and Clock

- Run the **clock set** command to configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

Updating the Hardware Clock

- If the hardware clock and software clock are not synchronized, run the **clock update-calendar** command to copy the date and time of the software clock to the hardware clock.

Configuring a System Name

- Run the **hostname** command to change the default system name.
- The default host name is **Ruijie**.

Configuring a Command Prompt

- Run the **prompt** command.

Configuring Daily Notification

- By default, no daily notification is configured.
- Run the **banner motd** command to configure daily notification.

- Daily notification is displayed on all terminals connected to network devices soon after login. Urgent messages (such as immediate system shutdown) can be delivered to users through daily notification.

Configuring a Login Banner

- By default, no login banner is configured.
- Run the **banner login** command to configure a login banner to display login information.

Configuring the Console Baud Rate

- Run the **speed** command.
- The default baud rate is 9,600 bps.

2.3.4 Displaying Configurations

Displays the system configurations, including the configurations that the system is currently running and the device configurations stored in the NVRAM.

Working Principle

Running Configurations

Running configurations, namely, running-config, are the configurations that individual component modules run in real time. A request can be made to all running components to collect configurations, which will be orchestrated before being displayed to users. Only running components may provide real-time configurations, whereas unloaded components do not display configurations. In the case that the system is started, a component process is restarted, and a hot patch is executed, the configurations collected during this period may be inaccurate due to the component unstable state. For example, the configurations of a component may not be missing initially but can be displayed later.

Startup Configurations

The configurations stored in the NVRAM, namely, startup-config, are the configurations executed during device startup. When the system is restarted, startup-config is loaded to become new running-config. To display permanent configurations, the system needs to read the **startup-config** file in the NVRAM.

Related Configuration

Displaying Running Configurations

Run the **show running-config** [**interface** *interface*] command to display the configurations that the system is currently running or the configurations on an interface.

Displaying Startup Configurations

Run the **show startup-config** command.

Storing Startup Configurations

Run the **write** or **copy running-config startup-config** command to store the current running configurations as new startup configurations.

2.3.5 Telnet

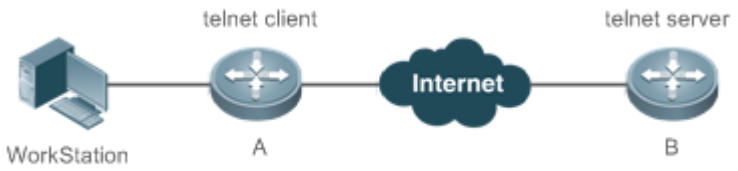
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol stack. It provides the standard governing remote login and virtual terminal communication on the internet.

The Telnet Client service allows a local or remote user who has logged in to a network device to use its Telnet Client program to access other remote system resources on the internet. In Figure 2-2, a user with a PC connects to Network Device A by using the terminal emulation or Telnet program and then logs in to Network Device B by using the **telnet** command to perform configuration management.

Ruijie Telnet program supports the use of IPv4 and IPv6 addresses. A Telnet server accepts Telnet connection requests that carry IPv4 and IPv6 addresses. A Telnet client can send connection requests to hosts identified by IPv4 and IPv6 addresses.

Figure 2-2



Related Configuration

Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

Restoring a Telnet Client Session

- Run the **<1-99>** command.

Disconnecting a Suspended Telnet Client Session

- Run the **disconnect** *session-id* command.

Enabling the Telnet Server Service

- Run the **enable service telnet-server** command.
- Perform this configuration when you need to enable Telnet login.

2.3.6 Restart

The timed restart feature makes user operation easier in some scenarios (such as tests).

- If you configure a time interval, the system will restart after the interval. The interval is in the format of *mmm* or *hhh:mm*, in the unit of minutes. You can specify the interval name to reflect the restart purpose.
- If you define a future time, the system will restart when the time is reached.

⚠ The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

⚠ The span between the restart time and current time must not exceed 31 days, and the restart time must be later than the current system time. After you configure a restart plan, do not to change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Configuration

Configuring Restart

- Run the **reload** command to configure a restart policy.
- Perform this configuration when you need to restart a device at a specific time.

2.3.7 Character Set Encoding

The character set encoding function enables the device to specify a unified character set encoding format. After a client enters a command in the CLI, the command is automatically converted into a command in the unified character set encoding format before delivery.

ℹ When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Related Configuration

Setting the Character Set Encoding Format

- Run the **language character-set { UTF-8 | GBK | default }** command to set the character set encoding format.
- The value **default** indicates that mixed codes are supported.

Displaying the Character Set Encoding Format

- Run the **show language character-set** command to display the current character set encoding format.

2.4 Configuration

Configuring Passwords and Privileges	⚠ (Optional) It is used to configure passwords and command privilege levels.	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.

	enable	Raises a user privilege level.
	disable	Lowers a user privilege level.
	privilege	Configures command privilege levels.
	password	Specifies a line password.
	login	Enables line password protection.
Configuring Login and Authentication	(Optional) It is used to configure different login modes and authentication methods.	
	username	Configures local user account information and optional authorization information.
	login local	Configures local authentication for line-based login.
	login authentication	Configures AAA authentication for line-based login.
	telnet	Enables the Telnet Client service.
	enable service telnet-server	Enables the Telnet Server service.
	exec-timeout	Configures the connection timeout time.
	session-timeout	Configures the session timeout time.
	lockable	Enables line-based terminal lock.
	lock	Locks a terminal connected to the current line.
Configuring Basic System Parameters	(Optional) It is used to configure basic system parameters.	
	clock set	Configures the system date and clock.
	clock update-calendar	Updates the hardware clock.
	hostname	Configures a system name.
	prompt	Configures a command prompt.
	banner motd	Configures daily notification.
	bannerlogin	Configures a login banner.
	speed	Configures the Console baud rate.
Enabling and Disabling a Specific Service	(Optional) It is used to enable and disable a specific service.	
	enable service	Enables a service.
Configuring a Restart Policy	(Optional) It is used to configure a system restart policy.	
	reload	Restarts a device.
Configuring Language Character Set	(Optional) It is used to configure the language character set.	
	language character-set { **UTF-8** | **GBK** | **default** }	Configures the language character set.

2.4.1 Configuring Passwords and Privileges

Configuration Effect

- Configure passwords to control users' access to network devices.
- Assign a privilege level to a command to grant the command access to only the users at or higher than the level.
- Lower the command privilege level to grant more users access to the command.
- Raise the command privilege level to limit the command access to a few users.

Notes

- You can use the password configuration command with the **level** option to configure a password for a specific privilege level. After you specify the level and the password, the password works for the users who need to access this level.
- By default, no password is configured for any level. The default level is 15.
- If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password.
- The system chooses the secure encrypted password over the simple encrypted password if both of them are configured.

Configuration Steps

↘ **Configuring a Simple Encrypted Password**

- (Optional) Perform this configuration when you need to establish simple encrypted password verification when users switch between different privilege levels.
- Run the **enable password** command to configure a simple encrypted password.

↘ **Configuring a Secure Encrypted Password**

- (Optional) Perform this configuration when you need to establish secure encrypted password verification when users switch between different privilege levels.
- Run the **enable secret** command to configure a secure encrypted password.
- A secure encrypted password has the same function as a simple encrypted password but uses an enhanced password encryption algorithm. Therefore, secure encrypted passwords are recommended out of security consideration.

↘ **Configuring Command Privilege Levels**

- Optional.
- A command at a lower level is accessible by more users than a command at a higher level.

↘ **Raising/Lowering a User Privilege Level**

- After logging in to a network device, the user can change his/her level to obtain access to commands at different privilege levels.

- Run the **enable** command or the **disable** command to raise or lower a user privilege level respectively.

Enabling Line Password Protection

- (Optional) Line password protection is required for remote login (such as login through Telnet).
- Run the **password** [**0** | **7**] *line* command to configure a line password, and then run the **login** command to enable login authentication.

If a line password is configured but login authentication is not configured, the system does not display password prompt.

Verification

- Run the **show privilege** command to display the current user level.
- Run the **show running-config** command to display the configuration.

Related Commands

Configuring a Simple Encrypted Password

Command	**enable password** [**level** *level*] { *password* | [**0** | **7**] *encrypted-password* }
Parameter Description	*level*: Indicates a specific user level. *password:* Indicates the password used to enter privileged EXEC mode. *0:* Indicates that the password is entered in plaintext. *7:* Indicates that the password is entered in cyphertext. *encrypted-password:* Indicates the password text, which must contain case-sensitive English letters and digits. Leading spaces are allowed, but will be ignored. However, intermediate and trailing spaces are recognized.
Command Mode	Global configuration mode
Usage Guide	Currently, simple encrypted passwords can be configured with only level 15 and take effect only when no secure encrypted password is configured. If you configure a simple encrypted password with a non-15 level, a warning is displayed and the password is automatically converted into a secure encrypted password. If the level 15 simple encrypted password and secure encrypted password are configured the same, a warning is displayed. If you specify an encryption type and enter a password in plaintext, you cannot re-enter privileged EXEC mode. An encrypted password cannot be retrieved once lost. You have to configure a new password.

Configuring a Secure Encrypted Password

Command	**enable secret** [**level** *level*] {*secret* | [**0 | 5**] *encrypted-secret* }

Parameter Description	*level*: Indicates a specific user level. secret: Indicates the password used to enter privileged EXEC mode. **0 | 5**: Indicates the password encryption type. 0 indicates no encryption, and 5 indicates secure encryption. *encrypted-password*: Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

Raising a User Privilege Level

Command	**enable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	An increase in privilege level requires the input of the target level password.

Lowering a User Privilege Level

Command	**disable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	A reduction in privilege level does not require password input. Use this command to exit Privileged EXEC mode and return to user EXEC mode. If *privilege-level* is specified, the current privilege level is reduced to the specified level. *privilege-level* must be lower than the current level.

Configuring Command Privilege Levels

Command	**privilege** *mode* [**all**] { **level** *level* | **reset** } *command-string*
Parameter Description	*mode*: Indicates the CLI mode of the command. For example, **config** indicates the global configuration mode, **EXEC** indicates the privileged command mode, and **interface** indicates the interface configuration mode. **all**: Changes the subcommand privilege levels of a specific command to the same level. **level** *level*: Indicates a privilege level, ranging from 0 to 15. **reset**: Restores the command privilege level to the default. *command-string*: Indicates the command to be assigned a privilege level.
Command Mode	Global configuration mode
Usage Guide	To restore a command privilege level, run the **no privilege** *mode* [**all**] **level** *level command* command in global configuration mode.

Specifying a Line Password

Command	**password**[**0** | **7**] *line*
Parameter Description	**0**: Indicates to configure a password in plaintext. **7**: Indicates to configure a password in cyphertext. line: Indicates the password string.
Command Mode	Line configuration mode
Usage Guide	N/A

Enabling Line Password Protection

Command	**login**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Configuring Command Authorization

Scenario	Assign privilege level 1 to the **reload** command and its subcommands and configure level 1 as the valid level (by configuring the **test** password).
Configuration Steps	● Assign privilege level 1 to the **reload** command and its subcommands.
	`Ruijie# configure terminal` `Ruijie(config)# privilege exec all level 1 reload` `Ruijie(config)# enable secret level 1 0 test` `Ruijie(config)# end`
Verification	● Check whether the **reload** command and its subcommands are accessible at level 1.
	`Ruijie# disable 1` `Ruijie> reload ?` `at reload at`

2.4.2 Configuring Login and Authentication

Configuration Effect

- Establish line-based login identity authentication.
- Run the **telnet** command on a network device to log in to a remote device.
- Close an established connection if no output is detected during the timeout time.
- Disconnect an established session connecting to a remote host and restore the host to Idle if no output is detected during the timeout time.
- Lock a terminal to deny access. When a user enters any character on the locked terminal, the password prompt is displayed. The terminal will be automatically unlocked if the entered password is correct.

Configuration Steps

Configuring Local User Information

- Mandatory.
- Run the **username** command to configure the account used for local identity authentication and authorization, including usernames, passwords, and optional authorization information.
- Perform this configuration on every device.

Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login in the case that AAA is disabled.
- Perform this configuration on every device.

Configuring AAA Authentication for Line-Based Login

- (Optional) Perform this configuration to configure AAA authentication for line-based login.
- Configure AAA authentication for line-based login in the case that AAA is enabled.
- Perform this configuration on every device.

Enabling the Telnet Client Service

- Run the **telnet** command to log in to a remote device.

Restoring a Telnet Client Connection

- (Optional) Perform this configuration to restore the connection on a Telnet client.

Closing a Suspended Telnet Client Connection

- (Optional) Perform this configuration to close the suspended connection on a Telnet client.

Enabling the Telnet Server Service

- Optional.
- Enable the Telnet Server service when you need to enable Telnet login.

Configuring the Connection Timeout Time

- Optional.
- An established connection will be closed if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the connection timeout time.

Configuring the Session Timeout Time

- Optional.
- The session connecting to a remote host will be disconnected and the host be restored to Idle if no output is detected during the timeout time.
- Perform this configuration when you need to increase or reduce the session timeout time.

Locking a Session

- (Optional) Perform this configuration when you need to temporarily exit a session on a device.
- To lock a session, first enable terminal lock in line configuration mode, and then run the **lock** command to lock the terminal.

Verification

- Run the **show running-config** command to display the configuration.
- In the case that AAA is disabled, after local user information and line-based local authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- In the case that AAA is enabled, after local user information and local AAA authentication are configured, check whether users are prompted for username and password input for access to the CLI.
- Run the **show user** command to display the information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet Server service.
- When a user presses **Enter** on a locked CLI, the user is prompted for password input. The session is unlocked only when the entered password is the same as the configured one.
- Run the **show sessions** command to display every established Telnet client instance.

Related Commands

Configuring Local User Information

Command	**username** *name* [**login mode** { **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string*]
Parameter Description	*name*: Indicates a user name. **login mode**: Indicates the login mode. **console**: Sets the login mode to Console. **ssh**: Sets the login mode to SSH.

	telnet: Sets the login mode to Telnet. **online amount** *number*: Indicates the maximum number of online accounts. **permission** *oper-mode path*: Configures the file operation permission. *op-mode* indicates the operation mode, and *path* indicates the directory or path of a specific file. **privilege** *privilege-level*: Indicates the account privilege level, ranging from 0 to 15. **reject remote-login**: Rejects remote login by using the account. **web-auth**: Allows only Web authentication for the account. **pwd-modify**: Allows the account owner to change the password. This option is available only when **web-auth** is configured. **nopassword**: Indicates that no password is configured for the account. **password** [**0** | **7**] *text-string*: Indicates the password configured for the account. 0 indicates that the password is input in plaintext, and 7 indicates that the password is input in cyphertext. The default is plaintext.
Command Mode	Global configuration mode
Usage Guide	Use this command to create a local user database to be used by authentication. If the value 7 is selected for the encryption type, the entered cyphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

Configuring Local Authentication for Line-Based Login

Command	**login local**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	Use this command to configure local authentication for line-based login in the case that AAA is disabled. Local user information is configured by using the **username** command.

Configuring AAA Authentication for Line-Based Login

Command	**login authentication** { **default** | *list-name* }
Parameter Description	**default:** Indicates the default authentication method list name. *list-name*: Indicates the optional method list name.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure AAA authentication for line-based login in the case that AAA is enabled. The AAA authentication methods, including RADIUS authentication, local authentication, and no authentication, are used during the authentication process.

Enabling the Telnet Client Service

Command	**telnet** *host* [*port*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }]
Parameter Description	*host*: Indicates the IPv4 address, IPv6 address, or host name of the Telnet server. *port*: Indicates the TCP port number of the Telnet server. The default value is 23. **/source:** Indicates the source IP address or source port used by a Telnet client. **ip** *A.B.C.D:* Indicates the source IPv4 address used by the Telnet client. **ipv6** *X:X:X:X::X:* Indicates the source IPv6 address used by the Telnet client. **interface** *interface-name*: Indicates the source port used by the Telnet client.
Command Mode	Privileged EXEC mode
Usage Guide	A user can telnet to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address.

Restoring a Telnet Client Session

Command	<1-99>
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	Use this command to restore a Telnet client session. A user can press the shortcut key **Ctrl**+**Shift**+**6 X** to temporarily exit the Telnet client session that is established using the **telnet** command, run the **<1-99>** command to restore the session, and run the **show sessions** command to display the session information.

Closing a Suspended Telnet Client Connection

Command	**disconnect** *session-id*
Parameter Description	*session-id*: Indicates the suspended Telnet client session ID.
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

Enabling the Telnet Server Service

Command	**enable service telnet-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the Telnet Server service. The IPv4 and IPv6 services are also enabled after the command is executed.

Configuring the Connection Timeout Time

Command	**exec-timeout** *minutes* [*seconds*]
Parameter Description	*minutes*: Indicates the connection timeout time in the unit of minutes. *seconds*: Indicates the connection timeout time in the unit of seconds.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the established connections on a line. A connection will be closed when no input is detected during the timeout time. To remove the connection timeout configuration, run the **no exec-timeout** command in line configuration mode.

Configuring the Session Timeout Time

Command	**session-timeout** *minutes*[**output**]
Parameter Description	*minutes*: Indicates the session timeout time in the unit of minutes. **output**: Indicates whether to add data output as a timeout criterion.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for the remote host sessions on a line. A session will be disconnected when no input is detected during the timeout time. To cancel the session timeout time, run the **no session-timeout** command in line configuration mode.

Enabling Line-Based Terminal Lock

Command	**lockable**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Locking a Terminal Connected to the Current Line

Command	**lock**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	N/A

Configuration Example

Establishing a Telnet Session to a Remote Network Device

Configuration Steps	● Establish a Telnet session to a remote network device with the IP address 192.168.65.119. ● Establish a Telnet session to a remote network device with the IPv6 address 2AAA:BBBB::CCCC.

	Ruijie# telnet 192.168.65.119 Trying 192.168.65.119 ... Open User Access Verification Password:
	Ruijie# telnet 2AAA:BBBB::CCCC Trying 2AAA:BBBB::CCCC ... Open User Access Verification Password:
Verification	● Check whether the Telnet sessions are established to the remote network devices.

Configuring the Connection Timeout Time

Configuration Steps	● Set the connection timeout time to 20 minutes.
	Ruijie# configure terminal//Enter global configuration mode. Ruijie# line vty 0 //Enter line configuration mode. Ruijie(config-line)#exec-timeout 20 //Set the connection timeout time to 20 minutes.
Verification	● Check whether the connection between a terminal and the local device is closed when no input is detected during the timeout time.

2.4.3 Configuring Basic System Parameters

Configuration Effect

- Configure basic system parameters.

Configuration Steps

Configuring the System Date and Clock

- Mandatory.
- Configure the system time of a network device manually. The device clock starts from the configured time and keeps running even when the device is powered off.

⚠ The time configuration is applied only to the software clock if the network device does not provide a hardware clock. The configuration will be invalid when the device is powered off.

Updating the Hardware Clock

- Optional.

- Perform this configuration when you need to copy the date and time of the software clock to the hardware clock so that the hardware clock is synchronized with the software clock.

Configuring a System Name

- (Optional) Perform this configuration to change the default system name.

Configuring a Command Prompt

- (Optional) Perform this configuration to change the default command prompt.

Configuring Daily Notification

- (Optional) Perform this configuration when you need to display important prompts or warnings to users.
- You can configure notification in one or multiple lines, which will be displayed to users after login.

Configuring a Login Banner

- (Optional) Perform this configuration when you need to display important messages to users upon login or logout.

Configuring the Console Baud Rate

- (Optional) Perform this configuration to change the default Console baud rate.

Verification

- Run the **show clock** command to display the system time.
- Check whether a login banner is displayed after login.
- Run the **show version** command to display the system information and version.

Related Commands

Configuring the System Date and Clock

Command	**clock set** *hh:mm:ss month day year*
Parameter Description	*hh:mm:ss*: Indicates the current time, in the format of *hour* (24-hour format):*minute*:*second*. *day*: Indicates a day (1–31) of the month. *month*: Indicates a month (from January to December) of the year. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to configure the system time. If the device does not provide a hardware clock, the time configuration will be invalid when the device is powered off.

Updating the Hardware Clock

Command	**clock update-calendar**

Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After the configuration, the time of the software clock will overwrite that of the hardware clock.

Configuring a System Name

Command	**hostname** *name*
Parameter Description	*name*: Indicates the system name, which must consist of printable characters and must not exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the system name to the default, run the **no hostname** command in global configuration mode.

Configuring a Command Prompt

Command	**prompt** *string*
Parameter Description	*string*: Indicates the command prompt name. A name with more than 32 characters will be truncated to keep only the first 32 characters.
Command Mode	Privileged EXEC mode
Usage Guide	To restore the command prompt to the default settings, run the **no prompt** command in global configuration mode.

Configuring Daily Notification

Command	**banner motd** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The message must not exceed 255 bytes.

Configuring a Login Banner

Command	**banner login** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as "&".
Command Mode	Global configuration mode
Usage Guide	A message must start and end with delimiter+carriage return respectively. Any characters following the ending delimiter will be dropped. Any letter contained in the message must not be used as the delimiter. The

	message must not exceed 255 bytes. To remove the login banner configuration, run the **no banner login** command in global configuration mode.

Configuring the Console Baud Rate

Command	**speed** *speed*
Parameter Description	*speed*: Indicates the console baud rate, in the unit of bps. The serial port baud rate can be set to 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps. The default is 9,600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate based on requirements. The **speed** command is used to configure receive and transmit rates for the asynchronous line.

Configuration Example

Configuring the System Time

Configuration Steps	● Change the system time to 2003-6-20, 10:10:12.
	`Ruijie# clock set 10:10:12 6 20 2003 //Configure the system time and date.`
Verification	● Run the **show clock** command in privileged EXEC mode to display the system time.
	`Ruijie# show clock //Confirm that the changed system time takes effect.` `clock: 2003-6-20 10:10:54`

Configuring Daily Notification

Configuration Steps	● Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	`Ruijie(config)# banner motd #//Starting delimiter` `Enter TEXT message. End with the character '#'.` `Notice: system will shutdown on July 6th.# //Ending delimiter` `Ruijie(config)#`
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	`C:\>telnet 192.168.65.236` `Notice: system will shutdown on July 6th.` `Access for authorized users only. Please enter your password.`

Configuration Steps	● Configure the daily notification message "Notice: system will shutdown on July 6th." with the pound key (#) as the delimiter.
	Ruijie(config)# banner motd #//Starting delimiter Enter TEXT message. End with the character '#'. Notice: system will shutdown on July 6th.# //Ending delimiter Ruijie(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether daily notification is displayed before the CLI appears.
	User Access Verification Password:

Configuring a Login Banner

Configuration Steps	● Configure the login banner message "Access for authorized users only. Please enter your password." with the pound key (#) as the delimiter.
	Ruijie(config)# banner login #//Starting delimiter Enter TEXT message. End with the character '#'. Access for authorized users only. Please enter your password. # //Ending delimiter Ruijie(config)#
Verification	● Run the **show running-config** command to display the configuration. ● Connect to the local device through the Console, Telnet or SSH, and check whether the login banner is displayed before the CLI appears.
	C:\>telnet 192.168.65.236 Notice: system will shutdown on July 6th. Access for authorized users only. Please enter your password. User Access Verification Password:

Configuring the Serial Port Baud Rate

Configuration Steps	● Set the serial port baud rate to 57,600 bps.

	Ruijie# configure terminal //Enter global configuration mode. Ruijie(config)# line console 0 //Enter console line configuration mode. Ruijie(config-line)# speed 57600 //Set the console baud rate to 57,600 bps. Ruijie(config-line)# end //Returns to privileged mode.
Verification	● Run the **show** command to display the configuration.
	Ruijie# show line console 0 //Displays the console configuration. CON Type speed Overruns * 0 CON 57600 0 Line 0, Location: "", Type: "vt100" Length: 25 lines, Width: 80 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never History is enabled, history size is 10. Total input: 22 bytes Total output: 115 bytes Data overflow: 0 bytes stop rx interrupt: 0 times Modem: READY

2.4.4 Enabling and Disabling a Specific Service

Configuration Effect

- Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP Agent, SSH Server, and Telnet Server).

Configuration Steps

↘ Enabling the SNMP Agent, SSH Server, and Telnet Server Services

- (Optional) Perform this configuration when you need to use these services.

Verification

- Run the **show running-config** command to display the configuration.
- Run the **show services** command to display the service Enabled/Disable state.

Related Commands

Enabling the SSH Server, Telnet Server, and SNMP Agent Services

Command	**enable service** { **ssh-server** | **telnet-server** | **snmp-agent** }
Parameter Description	**ssh-server:** Enables or disables the SSH Server service. The IPv4 and IPv6 services are also enabled together with this service. **telnet-server:** Enables or disables the Telnet Server service. The IPv4 and IPv6 services are also enabled together with this service. **snmp-agent:** Enables or disables the SNMP Agent service. The IPv4 and IPv6 services are also enabled together with this service.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable and disable specific services.

Configuration Example

Enabling the SSH Server Service

Configuration Steps	● Enable the SSH Server service.
	`Ruijie# configure terminal  //Enter global configuration mode.` `Ruijie(config)#enable service ssh-server  //Enable the SSH Server service.`
Verification	● Run the **show running-config** command to display the configuration. ● Run the **show ip ssh** command to display the configuration and running state of the SSH Server service.

2.4.5 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Steps

Configuring Direct Restart

Run the **reload** command in privileged EXEC mode to restart the system immediately.

Configuring Timed Restart

```
reload  at  hh:mm:ss month day year
```

If you configure a specific time, the system will restart at the time. The time must be a time in the future. The **month day year** parameter is optional. If it is not specified, the system clock time is used by default.

⚠ The clock feature must be supported by the system if you want to use the **at** option. It is recommended that you configure the system clock in advance. A new restart plan will overwrite the existing one. A restart plan will be invalid if the system is restarted before the plan takes effect.

⚠ The restart time must be later than the current system time. After you configure a restart plan, do not change the system clock; otherwise, the plan may fail (for example, the system time is changed to a time after the restart time.)

Related Commands

↘ Restarting a Device

Command	**reload** [**at** { *hh* [:*mm* [:*ss*]] } [*month* [*day* [*year*]]]]
Parameter Description	**at** *hh:mm:ss*: Indicates the time when the system will restart. *month*: Indicates a month of the year, ranging from 1 to 12. *day*: Indicates a date, ranging from 1 to 31. *year*: Indicates a year, ranging from 1993 to 2035. Abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

2.4.6 Configuring the Character Set Encoding Format

Configuration Effect

A unified character set encoding format is used on a device.

Notes

None

Configuration Steps

↘ Setting a Character Set Encoding Format

Run the **language character-set** command to set a character set encoding format.

⚠ When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Verification

Run the **show language character-set** command to display the specified character set encoding format.

Related Commands

Command	**language character-set** { **UTF-8** | **GBK** | **default** }
Parameter Description	**UTF-8**: Sets the character set encoding format to UTF-8. **GBK**: Sets the character set encoding format to GBK. **default**: Sets the character set encoding format to the default format (mixed codes supported).
Command Mode	Global configuration mode
Usage Guide	Run this command to use a unified character set encoding format on a device.

Common Errors

None

2.5 Monitoring

Displaying

Description	Command
show clock	Displays the current system time.
show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }	Displays line configurations.
show reload	Displays system restart settings.
show running-config [**interface** *interface*]	Displays the current running configurations of the device or the configurations on an interface.
show startup-config	Displays the device configurations stored in the NVRAM.
show this	Displays the current system configurations.
show sessions	Displays the information of each established Telnet client instance.
show language character-set	Displays the coded character set.

3 Configuring Lines

3.1 Overview

There are various types of terminal lines on network devices. You can manage terminal lines in groups based on their types. Configurations on these terminal lines are called line configurations. On network devices, terminal lines are classified into multiple types such as CTY, VTY.

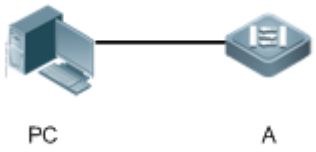
3.2 Applications

Application	Description
Accessing a Device Through Console	Enter the command-line interface (CLI) of a network device through the Console.
Accessing a Device Through VTY	Enter the CLI of a network device through Telnet or SSH.

3.2.1 Accessing a Device Through Console

Scenario

Figure 3-1



Remarks	A is a network device to be managed. PC is a network management station.

Deployment

The network management station connects to the Console port of a network device through a serial cable. Using the Console software (Hyper Terminal or other terminal simulation software) on the network management station, you can access the Console of the network device and enter the CLI to configure and manage the network device.

3.2.2 Accessing a Device Through VTY

Scenario

Figure 3-2

Remarks	A is a network device to be managed. PC is a network management station.

Deployment

The network management station connects to a network device through the network. Using a VTY client (such as Putty) on the network management station, you can access the network device through Telnet or SSH and enter the CLI to configure and manage the network device.

3.3 Features

Basic Concepts

CTY

The CTY line refers to the line connected to the Console port. Most network devices have a Console port. You can access the local system through the Console port.

VTY

The VTY line is a virtual terminal line that does not correspond to any hardware. It is used for Telnet or SSH connection.

Overview

Feature	Description
Basic Features	Configures a terminal, displays and clears terminal connection information.

3.3.1 Basic Features

Related Configuration

Clearing Terminal Connections

When a terminal connects to the network device, the corresponding terminal line is occupied. Run the **show user** command to display the connection status of these terminal lines. If you want to disconnect the terminal from the network device, run the **clear line** command to clear the terminal line. After the terminal lines are cleared, the related connections (such as Telnet and SSH) are interrupted, the CLI exits, and the terminal lines restore to the unoccupied status. Users can re-establish connections.

Specifying the Number of VTY Terminals

Run the **line vty** command to enter the VTY line configuration mode and specify the number of VTY terminals.

By default, there are 5 VTY terminals, numbered from 0 to 4. You can increase the number of VTY terminals to 36, with new ones numbered from 5 to 35. Only new terminals can be removed.

3.4 Configuration

Configuration	Description and Command	
Entering Line Configuration Mode	⚠ (Mandatory) It is used to enter the line configuration mode.	
	line [**console** | **vty**] *first-line* [*last-line*]	Enters the specified line configuration mode.
	line vty *line-number*	Increases or reduces the number of available VTY lines.

3.4.1 Entering Line Configuration Mode

Configuration Effect

Enter line configuration mode to configure other functions.

Configuration Steps

↘ Entering Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter line configuration mode on each device to configure line attributes.

↘ Increasing/Reducing the Number of VTY Lines

- Optional.
- Run the (**no**) **line vty** *line-number* command to increase or reduce the number of VTY lines.

Verification

Run the **show line** command to display line configuration.

Related Commands

↘ Entering Line Configuration Mode

Command	**line** [**console** | **vty**] *first-line* [*last-line*]
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *first-line*: Indicates the number of the first line. *last-line*: Indicates the number of the last line.
Command Mode	Global configuration mode

Usage Guide	N/A

Increasing/Reducing the Number of VTY Lines

Command	**line vty** *line-number*
Parameter Description	*line-number*: Indicates the number of VTY lines. The value ranges from 0 to 35.
Command Mode	Global configuration mode
Usage Guide	Run the **no line vty** *line-number* command to reduce the number of available VTY lines.

Displaying Line Configuration

Command	**show line** { **console** *line-num* | **vty** *line-num* **|** *line-num* }
Parameter Description	**console**: Indicates the Console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *line-num*: Indicates the line to be displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Scenario Figure 3-3	
Configuration Steps	● Connect the PC to network device A through the Console line and enter the CLI on the PC. ● Run the **show user** command to display the connection status of the terminal line. ● Run the **show line console** 0 command to display the status of the Console line. ● Enter global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
A	`Ruijie#show user` `Line User Host(s) Idle Location` `---------- ---------- ---------- ---------- ----------` `* 0 con 0 --- idle 00:00:00 ---`

```
Ruijie#show line console 0


CON     Type    speed   Overruns
* 0     CON     9600    0
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     ^D          ^M
Timeouts:      Idle EXEC    Idle Session
               00:10:00     never
History is enabled, history size is 10.
Total input: 490 bytes
Total output:  59366 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times


Ruijie#show line vty ?
  <0-5>    Line number


Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line vty 35
Ruijie(config-line)#
*Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
```

Verification

- After running the **show line** command, you can find that the number of terminals increases.
- Run the **show running-config** command to display the configuration.

A

```
Ruijie#show line vty ?
  <0-35>  Line number


Ruijie#show running-config
```

```
Building configuration...
Current configuration : 761 bytes


version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
line vty 0 35
 login
!
end
```

3.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the line connection status.	**clear line** { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }

Displaying

Description	Command
Displays the line configuration.	**show line** { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }
Displays historical records of a line.	**show history**
Displays the privilege level of a line.	**show privilege**
Displays users on a line.	**show user** [**all**]

4 Configuring RMON

4.1 Overview

The Remote Network Monitoring (RMON) aims at resolving problems of managing local area networks (LANs) and remote sites by using one central point. In RMON, network monitoring data consists of a group of statistics and performance indicators, which can be used for monitoring the network utilization, so as to facilitate network planning, performance optimization, and network error diagnosis.

RMON is mainly used by a managing device to remotely monitor and manage managed devices.

Protocols and Standards

STD 0059 / RFC 2819: Remote Network Monitoring Management Information Base

RFC4502: Remote Network Monitoring Management Information Base Version 2

RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)

RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules

RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms

RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions

RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services

RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks

RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros

RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

4.2 Applications

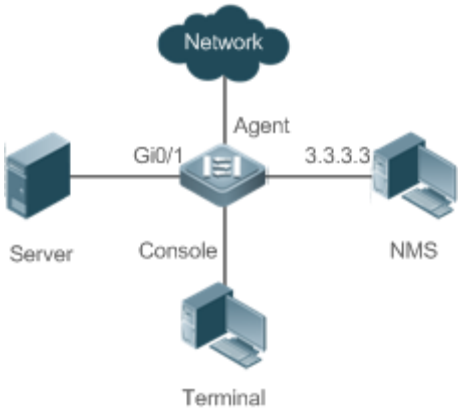
Application	Description
Collecting Statistics on Information of a Monitored Interface	Applies four functions of RMON to an interface to monitor the network communication of the interface.

4.2.1 Collecting Statistics on Information of a Monitored Interface

Scenario

The RMON Ethernet statistics function is used to monitor accumulated information of an interface, the history statistics function is used to monitor the packet count of an interface within each monitoring interval, and the alarm function is used to immediately acquire packet count exceptions of an interface. The following figure shows the networking topology.

Figure 4-1



Deployment

Interface x is monitored to accumulatively collect statistics on the packet count of the interface and collect statistics on the packet count and bandwidth utilization of the interface within the monitoring interval. If a packet count exception occurs on the interface, an alarm is reported to the network management system (NMS). The configuration key points are as follows:

- Configure the RMON Ethernet statistics function on interface x.
- Configure the RMON history statistics function on interface x.
- Configure the RMON alarm table and define RMON event processing actions in configuration mode. Monitored objects of alarms are the object identifier (OID) values of specific fields in the RMON Ethernet statistical table configured for interface x.

4.3 Features

Basic Concepts

RMON defines multiple RMON groups. Ruijie products support the statistics group, history group, alarm group, and event group, which are described as follows:

Statistics Group

The statistics group is used to monitor and collect statistics on Ethernet interface traffic information, which is accumulated from the entry creation time to the current time. The statistical items include discarded data packets, broadcast data packets, cyclic redundancy check (CRC) errors, large and small blocks, and collisions. Statistical results are stored in the Ethernet statistical table.

History Group

The history group is used to periodically collect network traffic information. It records accumulated values of network traffic information and the bandwidth utilization within each interval, and saves them in the history control table. It includes two small groups:

- The HistoryControl group is used to set the sampling interval, sampling data source, and other control information.

- The EthernetHistory group provides administrators with historical data, including statistics on network segment traffic, error packets, broadcast packets, utilization, and number of collisions.

Alarm Group

The alarm group is used to monitor a specified Management Information Base (MIB) object. When the value of a MIB object exceeds the preset upper limit or is lower than the preset lower limit, an alarm is triggered and the alarm is processed as an event.

Event Group

The event group is used to define the event processing mode. When a monitored MIB object meets alarm conditions, an event is triggered. An event can be processed in any of the following modes:

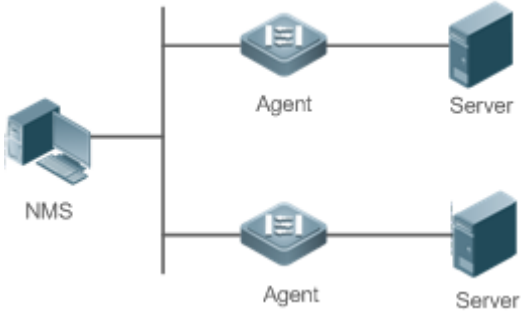
- none: No action is taken.
- log: Event-relevant information is recorded in the log record table so that administrators can view it at any time.
- snmp-trap: A trap message is transmitted to the NMS to notify the NMS of the event occurrence.
- log-and-trap: Event-relevant information is recorded in the log record table and a trap message is transmitted to the NMS.

Working Principle

RMON supports multiple monitors and two data collection methods. Method 1: A dedicated RMON probe is used to collect data and the NMS can directly acquire all information about the RMON MIB from the RMON probe. Method 2: RMON agents are built into network devices (such as switches and routers) so that the devices have the RMON probe function. The NMS uses basic commands of the Simple Network Management Protocol (SNMP) to exchange data with the RMON agents and collect network management information. This method, however, is limited by device resources and information of only four groups rather than all data of the RMON MIB is acquired.

The following figure shows an example of communication between the NMS and RMON agents. The NMS, through the RMON agents running on devices, can acquire information about overall traffic, error statistics, and performance statistics of the network segment where a managed network device interface is, thereby implementing remote management of network devices.

Figure 4-2



Overview

Feature	Description
RMON Ethernet Statistics	Collects statistics on the packet count, byte count, and other data of a monitored Ethernet interface accumulatively.
RMON History Statistics	Records the counts of packets, bytes, and other data communicated by an Ethernet interface within the configured interval and calculates the bandwidth utilization within the interval.
RMON Alarm	Samples values of monitored variables at intervals. The alarm table is used in combination with the event table. When the upper or lower limit is reached, a relevant event table is triggered to perform event processing or no processing is performed.

4.3.1 RMON Ethernet Statistics

Working Principle

The RMON Ethernet statistics function accumulatively collects statistics on network traffic information of an Ethernet interface from the entry creation time to the current time.

Related Configuration

↘ Configuring RMON Statistical Entries

- The RMON Ethernet statistics function is disabled by default.
- Run the **rmon collection stats** command to create Ethernet statistical entries on a specified Ethernet interface.
- After statistical entries are successfully created on a specified interface, the statistics group collects statistics on the traffic information of the current interface. The statistical items are variables defined in the RMON Ethernet statistical table, and recorded information is the accumulated values of variables from the creation time of the RMON statistical table to the current time.

4.3.2 RMON History Statistics

Working Principle

The RMON history statistics function records accumulated statistics on traffic information of an Ethernet interface within each interval.

Related Configuration

↘ Configuring RMON Historical Control Entries

- The RMON history statistics function is disabled by default.
- Run the **rmon collection history** command to create historical control entries on an Ethernet interface.
- The RMON history group collects statistics on variables defined in the RMON history table and records accumulated values of variables within each interval.

4.3.3 RMON Alarm

Working Principle

The RMON alarm function periodically monitors value changes of alarm variables. If the value of an alarm variable reaches the specified upper threshold or lower threshold, a corresponding event is triggered for processing, for example, a trap message is transmitted or one logTable entry record is generated. If a lower threshold or upper threshold is reached multiple times consecutively, only one corresponding event is triggered and another event is triggered till a reverse threshold is reached.

Related Configuration

Configuring the Event Table

- The RMON event group function is disabled by default.
- Run the **rmon event** command to configure the event table.

Configuring Alarm Entries

- The RMON alarm group function is disabled by default.
- Run the **rmon event** command to configure the event table and run the **rmon alarm** command to configure the RMON alarm table.
- The RMON alarm function is implemented by the alarm table and event table jointly. If a trap message needs to be transmitted to a managing device in the case of an alarm event, the SNMP agent must be correctly configured first. For the configuration of the SNMP agent, see the *Configuring SNMP*.
- If a configured alarm object is a field node in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function need to be configured on a monitored Ethernet interface first.

4.4 Configuration

Configuration	Description and Command	
Configuring RMON Ethernet Statistics	⚠ (Mandatory) It is used to accumulatively collect statistics on traffic information of an Ethernet interface.	
	rmon collection stats	Configures Ethernet statistical entries.
Configuring RMON History Statistics	⚠ (Mandatory) It is used to collect, at intervals, statistics on traffic information of an Ethernet interface and the bandwidth utilization within the interval.	
	rmon collection history	Configures historical control entries.
Configuring RMON Alarm	⚠ (Mandatory) It is used to monitor whether data changes of a variable is within the valid range.	
	rmon event	Configures event entries.

Configuration	Description and Command	
	rmon alarm	Configures alarm entries.

4.4.1 Configuring RMON Ethernet Statistics

Configuration Effect

Acquire accumulated statistics on traffic information of a monitored Ethernet interface from the entry creation time to the current time.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

↘ Configuring RMON Statistical Entries

- Mandatory.
- If statistics and monitoring are required for a specified interface, Ethernet statistical entries must be configured on this interface.

Verification

Run the **show rmon stats** command to display Ethernet statistics.

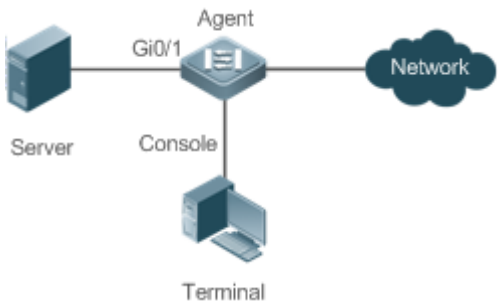
Related Commands

↘ Configuring RMON Statistical Entries

Command	**rmon collection stats** *index* [**owner** *ownername*]
Parameter Description	*index*: Indicates the index number of a statistical entry, with the value ranging from 1 to 65,535. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.
Command Mode	Interface configuration mode
Usage Guide	The values of statistical entry parameters cannot be changed.

Configuration Example

↘ Configuring RMON Ethernet Statistics

Scenario **Figure 4-3**	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS requires the RMON statistics group to conduct performance statistics on received packets of interface Gi0/1. Administrators can view the statistics at any time to understand data about received packets of an interface and take measures in a timely manner to handle network exceptions.
Configuration Steps	● Configure a statistical table instance on interface GigabitEthernet 0/1 to collect statistics on the traffic of this interface.
Agent	`Ruijie# configure terminal` `Ruijie (config)# interface gigabitEthernet 0/1` `Ruijie (config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin`
Verification	Run the **show rmon stats** command to display Ethernet statistics.
Agent	`Ruijie# show rmon stats` `ether statistic table:` `index = 1` `interface = GigabitEthernet 0/1` `owner = admin` `status = 1` `dropEvents = 0` `octets = 25696` `pkts = 293` `broadcastPkts = 3` `multiPkts = 0` `crcAlignErrors = 0` `underSizePkts = 0` `overSizePkts = 0` `fragments = 0`

	jabbers = 0 collisions = 0 packets64Octets = 3815 packets65To127Octets = 1695 packets128To255Octets = 365 packets256To511Octets = 2542 packets512To1023Octets = 152 packets1024To1518Octets = 685

Common Errors

Statistical table entries are re-configured or configured statistical table entries are modified.

4.4.2 Configuring RMON History Statistics

Configuration Effect

Acquire accumulated statistics on the traffic of a monitored Ethernet interface and the bandwidth utilization within each interval.

Notes

This function cannot be configured in batch interface configuration mode.

Configuration Steps

- Mandatory.
- If network statistics on a specified interface need to be collected, RMON historical control entries must be configured on the interface.

Verification

Run the **show rmon history** command to display history group statistics.

Related Commands

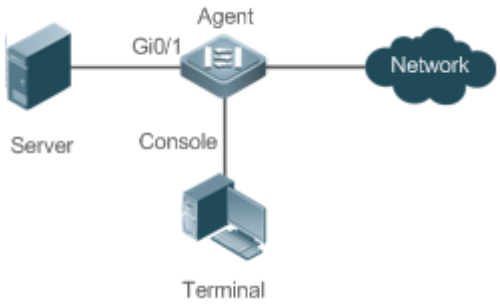
↘ Configuring RMON Historical Control Entries

Command	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
Parameter Description	*index*: Indicates the index number of a history statistical entry, with the value ranging from 1 to 65,535. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters. **buckets** *bucket-number*: Sets the capacity of the history table in which a history statistical entry exists, that is, sets the maximum number of records (*bucket-number*) that can be accommodated in the history table.

	The value of *bucket-number* ranges from 1 to 65,535 and the default value is **10**. **interval** *seconds*: Sets the statistical interval, with the unit of seconds. The value ranges from 1 second to 3,600 seconds and the default value is **1,800** seconds.
Command Mode	Interface configuration mode
Usage Guide	The values of history statistical entry parameters cannot be changed.

Configuration Example

Configuring RMON History Statistics

Scenario Figure 4-4	
	As shown in the preceding figure, the RMON agent is connected to the server, and the NMS needs to collect statistics on received packets of interface Gi0/1 through the RMON history group at an interval of 60 seconds, in an effort to monitor the network and understand emergency data.
Configuration Steps	● Configure the history control table on interface GigabitEthernet 0/1 to periodically collect statistics on the traffic of this interface.
Agent	`Ruijie# configure terminal` `Ruijie(config)# interface gigabitEthernet 0/1` `Ruijie(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5 interval 300 owner admin`
Verification	Run the **show rmon history** command to display history group statistics.
Agent	`Ruijie# show rmon history` `rmon history control table:` `index = 1` `interface = GigabitEthernet 0/1` `bucketsRequested = 5` `bucketsGranted = 5` `interval = 60` `owner = admin`

```
                    stats = 1


rmon history table:
                    index = 1
                    sampleIndex = 786
                    intervalStart = 6d:18h:37m:38s
                    dropEvents = 0
                    octets = 2040
                    pkts = 13
                    broadcastPkts = 0
                    multiPkts = 0
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0

                    index = 1
                    sampleIndex = 787
                    intervalStart = 6d:18h:38m:38s
                    dropEvents = 0
                    octets = 1791
                    pkts = 16
                    broadcastPkts = 1
                    multiPkts = 0
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
```

```
collisions = 0
utilization = 0

index = 1
sampleIndex = 788
intervalStart = 6d:18h:39m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 789
intervalStart = 6d:18h:40m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
```

```
                collisions = 0
                utilization = 0


                index = 1
                sampleIndex = 790
                intervalStart = 6d:18h:41m:38s
                dropEvents = 0
                octets = 86734
                pkts = 934
                broadcastPkts = 32
                multiPkts = 23
                crcAlignErrors = 0
                underSizePkts = 0
                overSizePkts = 0
                fragments = 0
                jabbers = 0
                collisions = 0
                utilization = 0
```

Common Errors

History control table entries are re-configured or configured history control table entries are modified.

4.4.3 Configuring RMON Alarm

Configuration Effect

Periodically monitor whether value changes of alarm variables are within the specified valid range.

Notes

If a trap message needs to be transmitted to a managing device when an alarm event is triggered, the SNMP agent must be correctly configured. For the configuration of the SNMP agent, see the *Configuring SNMP*.

If an alarm variable is a MIB variable defined in the RMON statistics group or history group, the RMON Ethernet statistics function or RMON history statistics function must be configured on the monitored Ethernet interface. Otherwise, an alarm table fails to be created.

Configuration Steps

Configuring Event Entries

- Mandatory.
- Complete the configuration in global configuration mode.

Configuring Alarm Entries

- Mandatory.
- Complete the configuration in global configuration mode.

Verification

- Run the **show rmon event** command to display the event table.
- Run the **show rmon alarm** command to display the alarm table.

Related Commands

Configuring the Event Table

Command	**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an event table, with the value ranging from 1 to 65,535. **log**: Indicates a log event. The system logs a triggered event. **trap** *community*: Indicates a trap event. When an event is triggered, the system transmits a trap message with the community name of *community*. **description** d*escription-string*: Sets the description information about an event, that is, *description-string*. The value is a string of 1-127 characters. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.
Command Mode	Global configuration mode
Usage Guide	The values of configured event entry parameters can be changed, including the event type, trap community name, event description, and event creator.

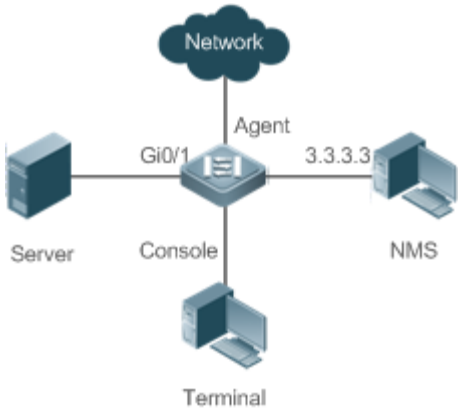
Configuring the RMON Alarm Group

Command	**rmon alarm** *number variable interval* {**absolute	delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]
Parameter Description	*number*: Indicates the index number of an alarm entry, with the value ranging from 1 to 65,535. *variable*: Indicates an alarm variable, which is a string of 1-255 characters and is represented in dotted format using the node OID (format: entry.integer.instance; example: 1.3.6.1.2.1.2.1.10.1). *Interval*: Indicates the sampling interval, with the unit of seconds and the value ranging from 1 to 2,147,483,647. **absolute**: Indicates that the sampling type is absolute value sampling, that is, variable values are directly extracted when the sampling time is up. **delta**: Indicates that the sampling type is changing value sampling, that is, changes in the variable values

	within the sampling interval are extracted when the sampling time is up. **rising-threshold** *value*: Sets the upper limit of the sampling quantity (*value*), with the value ranging from -2,147,483,648 to +2,147,483,647. *event-number:* Indicates that an event with the event number of *event-number* is triggered when the upper limit or lower limit is reached. **falling-threshold** *value*: Sets the lower limit of the sampling quantity (*value*), with the value ranging from -2,147,483,648 to +2,147,483,647. **owner** *ownername*: Indicates the entry creator, that is, *ownername*, which is a case-sensitive string of 1-63 characters.
Command Mode	Global configuration mode
Usage Guide	Values of configured alarm entry parameters can be changed, including alarm variables, sampling type, entry creator, sampling interval, upper/lower limit of the sampling quantity, and relevant trigger events.

Configuration Example

Configuring RMON Alarm

Scenario **Figure 4-5**	
	Assume that SNMPv1 runs on the NMS, the community name used for accessing the settings is public, with the attribute of read-write, and the IP address used by the NMS to receive trap messages is 3.3.3.3. Assume that the OID value of unknown protocol packets received by monitored interface GigabitEthernet0/3 is 1.3.6.1.2.1.2.2.1.15.3, the sampling mode is relative sampling, and the sampling interval is 60 seconds. When the relative sampling value is larger than 100 or lower than 10, event 1 and event 2 are triggered respectively. In event 1, a trap message is transmitted and the event is logged. In event 2, the event is only logged. The configuration of the RMON agent is completed on the terminal. The RMON agent is connected to the NMS and is connected to the server through interface GI0/1. The RMON agent needs to monitor the count of unknown protocol packets received by interface GI0/1. The sampling interval is 60 seconds. When the absolute sampling value is smaller than 10, the event is only logged. When the absolute sampling value is larger than 100, the event is logged and a trap message is transmitted to the NMS.
Configuration	● Configure the host address for receiving trap messages.

Steps	● Configure an event group to process alarm trigger. ● Configure the alarm function.
Agent	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# snmp-server community public rw Ruijie(config)# snmp-server host 3.3.3.3 trap public Ruijie(config)# rmon event 1 description rising-threshold-event log trap public owner admin Ruijie(config)# rmon event 2 description falling-threshold-event log owner admin Ruijie(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-threshold 10 2 owner admin
Verification	● Run the **show rmon event** command to display the event table. ● Run the **show rmon alarm** command to display the alarm table.
Agent	Ruijie# show rmon event rmon event table: index = 1 description = rising-threshold-event type = 4 community = public lastTimeSent = 0d:0h:0m:0s owner = admin status = 1 index = 2 description = falling-threshold-event type = 2 community = lastTimeSent = 6d:19h:21m:48s owner = admin status = 1 rmon log table:

```
                    eventIndex = 2
                    index = 1
                    logTime = 6d:19h:21m:48s
                    logDescription = falling-threshold-event
Ruijie# show rmon alarm
rmon alarm table:
            index: 1,
            interval: 60,
            oid = 1.3.6.1.2.1.2.2.1.15.3
            sampleType: 2,
            alarmValue: 0,
            startupAlarm: 3,
            risingThreshold: 100,
            fallingThreshold: 10,
            risingEventIndex: 1,
            fallingEventIndex: 2,
            owner: admin,
            stauts: 1
```

Common Errors

- The entered OID of a monitored object is incorrect, the variable corresponding to the OID does not exist, or the type is not an integer or unsigned integer.
- The upper threshold is smaller than or equal to the lower threshold.

4.5 Monitoring

Displaying

Description	Command
Displays all RMON configuration information.	**show rmon**
Displays the Ethernet statistical table.	**show rmon stats**
Displays the history control table.	**show rmon history**
Displays the alarm table.	**show rmon alarm**
Displays the event table.	**show rmon event**

5 Configuring SNMP

5.1 Overview

Simple Network Management Protocol (SNMP) became a network management standard RFC1157 in August 1988. At present, because many vendors support SNMP, SNMP has in fact become a network management standard and is applicable to the environment where systems of multiple vendors are interconnected. By using SNMP, the network administrator can implement basic functions such as information query for network nodes, network configuration, fault locating, capacity planning, and network monitoring and management.

↘ SNMP Versions

Currently, the following SNMP versions are supported:

- SNMPv1: The first official version of SNMP, which is defined in RFC1157.
- SNMPv2C: Community-based SNMPv2 management architecture, which is defined in RFC1901.
- SNMPv3: SNMPv3 provides the following security features by identifying and encrypting data.

4. Ensuring that data is not tampered during transmission.
5. Ensuring that data is transmitted from legal data sources.
6. Encrypting packets and ensuring data confidentiality.

Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419, Textual Conventions for Transport Addresses

5.2 Applications

Application	Description
Managing Network Devices Based on SNMP	Network devices are managed and monitored based on SNMP.

5.2.1 Managing Network Devices Based on SNMP

Scenario

Take the following figure as an example. Network device A is managed and monitored based on SNMP network manager.

Figure 5-1

Remarks	A is a network device that needs to be managed. PC is a network management station.

Deployment

The network management station is connected to the managed network devices. On the network management station, users access the Management Information Base (MIB) on the network devices through the SNMP network manager and receive messages actively sent by the network devices to manage and monitor the network devices.

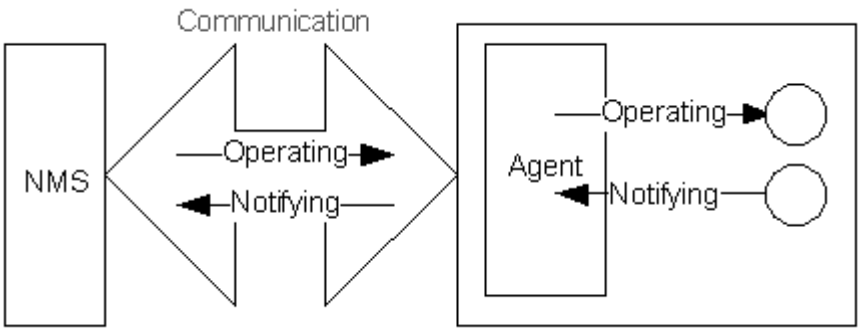
5.3 Features

Basic Concepts

SNMP is an application layer protocol that works in C/S mode. It consists of three parts:

- SNMP network manager
- SNMP agent
- MIB

Figure 5-2 shows the relationship between the network management system (NMS) and the network management agent.



SNMP Network Manager

The SNMP network manager is a system that controls and monitors the network based on SNMP and is also called the NMS.

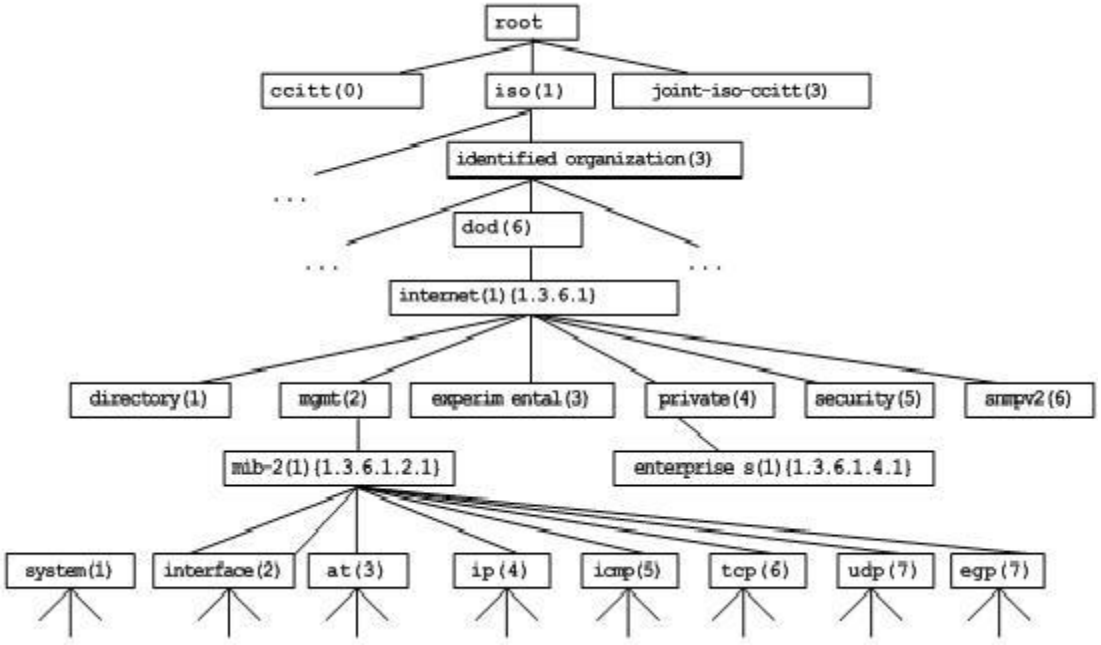
SNMP Agent

The SNMP agent (hereinafter referred to as the agent) is software running on the managed devices. It is responsible for receiving, processing, and responding to monitoring and control packets from the NMS. The agent may also actively send messages to the NMS.

MIB

The MIB is a virtual network management information base. The managed network devices contain lots of information. To uniquely identify a specific management unit among SNMP packets, the MIB adopts the tree hierarchical structure. Nodes in the tree indicate specific management units. A string of digits may be used to uniquely identify a management unit system among network devices. The MIB is a collection of unit identifiers of network devices.

Figure 5-3 Tree Hierarchical Structure



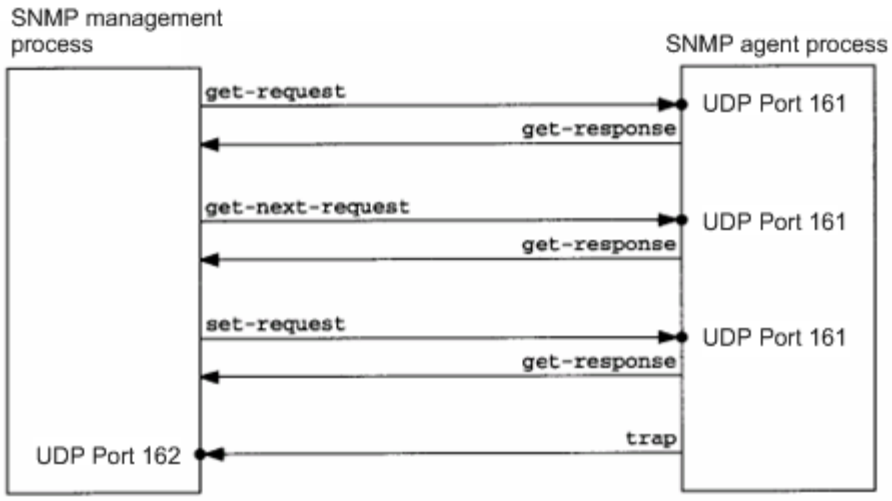
Operation Types

Six operation types are defined for information exchange between the NMS and the agent based on SNMP:

- Get-request: The NMS extracts one or more parameter values from the agent.
- Get-next-request: The NMS extracts the parameter value next to one or more parameters from the agent.
- Get-bulk: The NMS extracts a batch of parameter values from the agent.
- Set-request: The NMS sets one or more parameter values of the agent.
- Get-response: The agent returns one or more parameter values, which are the operations in response to the three operations performed by the agent on the NMS.
- Trap: The agent actively sends a message to notify the NMS of something that happens.

The first four packets are sent by the NMS to the agent and the last two packets are sent by the agent to the NMS. (Note: SNMPv1 does not support the Get-bulk operation.) Figure 5-4 describes the operations.

Figure 5-4 SNMP Packet Types



The three operations performed by the NMS on the agent and the response operations of the agent are based on UDP port 161. The trap operation performed by the agent is based on UDP port 162.

Overview

Feature	Description
Basic SNMP Functions	The SNMP agent is configured on network devices to implement basic functions such as information query for network nodes, network configuration, fault locating, and capacity planning.
SNMPv1 and SNMPv2C	SNMPv1 and SNMPv2C adopt the community-based security architecture, including authentication name and access permission.
SNMPv3	SNMPv3 redefines the SNMP architecture, namely, it enhances security functions, including the security model based on users and access control model based on views. The SNMPv3 architecture already includes all functions of SNMPv1 and SNMPv2C.

5.3.1 Basic SNMP Functions

Working Principle

Working Process

SNMP protocol interaction is response interaction (for exchange of packets, see Figure 5-4). The NMS actively sends requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. The agent receives the requests, completes operations, and returns a Get-response. Sometimes, the agent actively sends a trap message and an Inform message to the NMS. The NMS does not need to respond to the trap message but needs to return an Inform-response to the agent. Otherwise, the agent re-sends the Inform message.

Related Configuration

Shielding or Disabling the SNMP Agent

By default, the SNMP function is enabled.

The **no snmp-server** command is used to disable the SNMP agent.

The **no enable service snmp-agent** command is used to directly disable all SNMP services.

Setting Basic SNMP Parameters

By default, the system contact mode, system location, and device Network Element (NE) information are empty. The default serial number is 60FF60, the default maximum packet length is 1,572 bytes, and the default UDP port ID of the SNMP service is 161.

The **snmp-server contact** command is used to configure or delete the system contact mode.

The **snmp-server location** command is used to configure or delete the system location.

The **snmp-server chassis-id** command is used to configure the system serial number or restore the default value.

The **snmp-server packetsize** command is used to configure the maximum packet length of the agent or restore the default value.

The **snmp-server net-id** command is used to configure or delete the device NE information.

The **snmp-server udp-port** command is used to set the UDP port ID of the SNMP service or restore the default value.

Configuring the SNMP Host Address

By default, no SNMP host is configured.

The **snmp-server host** command is used to configure the NMS host address to which the agent actively sends messages or to delete the specified SNMP host address. In the messages sent to the host, the SNMP version, receiving port, authentication name, or user can be bound. This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

Setting Trap Message Parameters

By default, SNMP is not allowed to actively send a trap message to the NMS, the function of sending a Link Trap message on an interface is enabled, the function of sending a system reboot trap message is disabled, and a trap message does not carry any private field.

By default, the IP address of the interface where SNMP packets are sent is used as the source address.

By default, the length of a trap message queue is 10 and the interval for sending a trap message is 30s.

The **snmp-server enable traps** command is used to enable or disable the agent to actively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable or disable the function of sending a Link Trap message on an interface.

The **snmp-server trap-source** command is used to specify the source address for sending messages or to restore the default value.

The **snmp-server queue-length** command is used to set the length of a trap message queue or to restore the default value.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message or to restore the default value.

The **snmp-server trap-format private** command is used to set or disable the function of carrying private fields in a trap message when the message is sent.

The **snmp-server system-shutdown** command is used to enable or disable the function of sending a system reboot trap message.

↘ Setting the SNMP Attack Protection and Detection Function

By default, the SNMP attack protection and detection function is disabled.

The **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** } command is used to set and enable the attack protection and detection function.

5.3.2 SNMPv1 and SNMPv2C

SNMPv1 and SNMPv2C adopt the community-based security architecture. The administrator who can perform operations on the MIB of the agent is limited by defining the host address and authentication name (community string).

Working Principle

SNMPv1 and SNMPv2 determine whether the administrator has the right to use MIB objects by using the authentication name. The authentication name of the NMS must be the same as an authentication name defined in devices.

SNMPv2C adds the Get-bulk operation mechanism and can return more detailed error message types to the management workstation. The Get-bulk operation is performed to obtain all information from a table or obtain lots of data at a time, so as to reduce the number of request responses. The enhanced error handling capabilities of SNMPv2C include extension of error codes to differentiate error types. In SNMPv1, however, only one error code is provided for errors. Now, errors can be differentiated based on error codes. Because management workstations supporting SNMPv1 and SNMPv2C may exist on

the network, the SNMP agent must be able to identify SNMPv1 and SNMPv2C packets and return packets of the corresponding versions.

Security

One authentication name has the following attributes:

- Read-only: Provides the read permission of all MIB variables for authorized management workstations.
- Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Related Configuration

Setting Authentication Names and Access Permissions

The default access permission of all authentication names is read-only.

The **snmp-server community** command is used to configure or delete an authentication name and access permission.

This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed.

5.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2 into the SNMPv3 system.

Working Principle

The NMS and SNMP agent are SNMP entities. In the SNMPv3 architecture, SNMP entities consist of the SNMP engine and SNMP applications. The SNMP engine is used to send and receive messages, identify and encrypt information, and control access to managed objects. SNMP applications refer to internal applications of SNMP, which work by using the services provided by the SNMP engine.

SNMPv3v determines whether a user has the right to use MIB objects by using the User-based Security Model (USM). The security level of the NMS user must be the same as that of an SNMP user defined in devices so as to manage devices.

SNMPv3 requires the NMS to obtain the SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not know agent engine IDs, the NMS may first send a discover message to the agent and the agent returns a report message carrying an engine ID. Later, management operations between the NMS and the agent must carry the engine ID.

Security

- SNMPv3 determines the data security mechanism based on the security model and security level. At present, security models include: SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

SNMPv1 and SNMPv2C Security Models and Security Levels

Security Model	Security Level	Authentication	Encryption	Description

SNMPv1	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed through authentication name.

SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed through user name.
SNMPv3	authNoPriv	MD5 or SHA	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5 or SHA	DES	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA and data encryption mechanism based on CBC-DES are provided.

Engine ID

An engine ID is used to uniquely identify an SNMP engine. Because each SNMP entity includes only one SNMP engine, one SNMP engine uniquely identifies an SNMP entity in a management domain. Therefore, the SNMPv3 agent as an entity must has a unique engine ID, that is, SnmpEngineID.

An engine ID is an octet string that consists of 5 to 32 bytes. RFC3411 defines the format of an engine ID:

- The first four bytes indicate the private enterprise ID (allocated by IANA) of a vendor, which is expressed in hexadecimal.
- The fifth byte indicates remaining bytes:
- 0: Reserved.
- 1: The later four bytes indicate an IPv4 address.
- 2: The later 16 bytes indicate an IPv6 address.
- 3: The later six bytes indicate a MAC address.
- 4: Text consisting of 27 bytes, which is defined by the vendor.
- 5: Hexadecimal value consisting of 27 bytes, which is defined by the vendor.
- 6-127: Reserved.
- 128-255: Formats specified by the vendor.

Related Configuration

Configuring an MIB View and a Group

By default, one view is configured and all MIB objects can be accessed.

By default, no user group is configured.

The **snmp-server view** command is used to configure or delete a view and the **snmp-server group** command is used to configure or delete a user group.

One or more instructions can be configured to specify different community names so that network devices can be managed by NMSs of different permissions.

↘ Configuring an SNMP User

By default, no user is configured.

The **snmp-server user** command is used to configure or delete a user.

The NMS can communicate with the agent by using only legal users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (only DES is available currently), and encryption password.

5.3.4 SNMP MIB Cache Function

In unified management mode with multiple devices virtualized into one, the NMS needs to collect MIB variables on the slave/backup device via the master device. The whole collection process takes a long time if there are many devices.

Working Principle

The SNMP MIB cache function can be enabled to reduce the time consumed by the whole collection process. This function enables the master device to collect MIB variables on the slave/backup device in advance and cache the collected MIB variables. In this way, the NMS can directly read the cached MIB variables from the master device, avoid accessing the slave/backup device and reducing the consumed time.

Related Configuration

↘ Configuring SNMP MIB Cache Function

The SNMP MIB cache function is disabled by default.

Run the **snmp-server cache enable** command to configure the SNMP MIB cache function.

↘ Configuring SNMP MIB Cache Update Interval

The cache update interval is 300 seconds by default.

Run the **snmp-server cache update-timer** *seconds* command to configure the SNMP MIB cache update interval.

↘ Enabling Cache Function on Node with Specified OID and Configuring Cache Update Interval of This Node

The MIB cache function is disabled by default. The cache update interval of a node with a specified object identifier (OID) is consistent with the global cache update interval by default.

Run the **snmp-server cache oid** *oid-string* [**update-timer** *seconds*] command to enable the cache function on a node with a specified OID and configure the cache update interval of this node.

5.4 Configuration

Configuration	Description and Command	
Configuring Basic SNMP Functions	(Mandatory) It is used to enable users to access the agent through the NMS.	
	enable service snmp-agent	Enables the agent function.
	snmp-server community	Sets an authentication name and access permission.
	snmp-server user	Configures an SNMP user.
	snmp-server view	Configures an SNMP view.
	snmp-server group	Configures an SNMP user group.
	snmp-server authentication	Configures the SNMP attack protection and detection function.
Enabling the Trap Function	(Optional) It is used to enable the agent to actively send a trap message to the NMS.	
	snmp-server host	Configures the NMS host address.
	snmp-server enable traps	Enables the agent to actively send a trap message to the NMS.
	snmp trap link-status	Enables the function of sending a Link Trap message on an interface.
	snmp-server system-shutdown	Enables the function of sending a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server trap-format private	Enables a trap message to carry private fields when the message is sent.
Shielding the Agent Function	(Optional) It is used to shield the agent function when the agent service is not required.	
	no snmp-server	Shields the agent function.
Setting SNMP Control Parameters	(Optional) It is used to set or modify SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.
	snmp-server chassis-id	Sets the serial number of the device.
	snmp-server net-id	Sets NE information about the device.
	snmp-server packetsize	Modifies the maximum packet length.
	snmp-server udp-port	Modifies the UDP port ID of the SNMP service.
	snmp-server queue-length	Modifies the length of a trap message queue.
	snmp-server trap-timeout	Modifies the interval for sending a trap message.

Configuration	Description and Command	
Configuring SNMP MIB Cache Function	(Optional) It is used to set or modify the SNMP MIB cache function.	
	snmp-server cache enable	Configures the global SNMP MIB cache function.
	snmp-server cache update-timer	Configures the global SNMP MIB cache update interval.
	snmp-server cache oid	Enables the cache function on a node with a specified OID and configures the cache update interval of this node.

5.4.1 Configuring Basic SNMP Functions

Configuration Effect

Enable users to access the agent through the NMS.

Notes

- By default, no authentication name is set on network devices and SNMPv1 or SNMPv2C cannot be used to access the MIB of network devices. When an authentication name is set, if no access permission is specified, the default access permission is read-only.

Configuration Steps

Configuring an SNMP View

- Optional
- An SNMP view needs to be configured when the View-based Access Control Model (VACM) is used.

Configuring an SNMP User Group

- Optional
- An SNMP user group needs to be configured when the VACM is used.

Configuring an Authentication Name and Access Permission

- Mandatory
- An authentication name must be set on the agent when SNMPv1 and SNMPv2C are used to manage network devices.

Configuring an SNMP User

- Mandatory
- A user must be set when SNMPv3 is used to manage network devices.

Enabling the Agent Function

- Optional
- By default, the agent function is enabled. When the agent function needs to be enabled again after it is disabled, this command must be used.

Enabling the SNMP Attack Protection and Detection Function

- Optional
- By default, the SNMP attack protection and detection function is disabled. When malicious attacks need to be prevented, the configuration item must be used on the agent.

Verification

Run the **show snmp** command to check the SNMP function on devices.

Related Commands

Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: View name *oid-tree*: MIB objects associated with a view, which are displayed as an MIB subtree. **include:** Indicates that the MIB object subtree is included in the view. **exclude:** Indicates that the MIB object subtree is not included in the view.
Command Mode	Global configuration mode
Usage Guide	Specify a view name and use it for view-based management.

Configuring an SNMP User Group

Command	**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	**v1** | **v2c** |**v3:** Specifies the SNMP version. **auth:** Messages sent by users in the group need to be verified but data confidentiality is not required. This configuration is valid for SNMPv3 only. **noauth:** Messages sent by users in the group do not need to be verified and data confidentiality is not required. This configuration is valid for SNMPv3 only. **priv:** Messages sent by users in the group need to be verified and confidentiality of transmitted data is required. This configuration is valid for SNMPv3 only. *readview*: Associates one read-only view. *writeview*: Associates one read/write view. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which

	access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Associate certain users with a group and associate the group with a view. Users in a group have the same access permission. In this way, you can determine whether managed objects associated with an operation are in the allowable range of a view. Only managed objects in the range of a view can be accessed.

Configuring an Authentication Name and Access Permission

Command	**snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a plaintext string. *7*: Indicates that the input community string is a ciphertext string. *string*: Community string, which is equivalent to the communication password between the NMS and the SNMP agent. *view-name*: Specifies a view name for view-based management. **ro:** Indicates that the NMS can only read variables of the MIB. **rw:** The NMS can read and write variables of the MIB. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified. *ipaddr*: Associates NMS addresses and specifies NMS addresses for accessing the MIB.
Command Mode	Global configuration mode
Usage Guide	This command is the first important command for enabling the SNMP agent function. It specifies community attributes and NMS scope where access to the MIB is allowed. To disable the SNMP agent function, run the **no snmp-server** command.

Configuring an SNMP User

Command	**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]
Parameter Description	*username*: User name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3:** Specifies the SNMP version. Only SNMPv3 supports later security parameters. **encrypted:** The specified password input mode is ciphertext input. Otherwise, plaintext is used for input. If ciphertext input is selected, enter a key consisting of continuous hexadecimal digits. An MD5 protocol authentication key consists of 16 bytes and an SHA authentication protocol key consists of 20 bytes. Two

	characters stand for one byte. Encrypted keys are valid for this engine only. **auth:** Specifies whether authentication is used. **md5:** Specifies the MD5 authentication protocol. **sha** specifies the SHA authentication protocol. *auth-password*: Configures a password string (not more than 32 characters) used by the authentication protocol. The system converts the passwords into the corresponding authentication keys. **priv:** Specifies whether confidentiality is used. **des56** specifies the use of the 56-bit DES encryption protocol. *priv-password*: Configures a password string (not more than 32 characters) used for encryption. The system converts the password into the corresponding encryption key. *aclnum*: ACL number. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *aclname*: ACL name. The specified ACL is associated and the range of IPv4 NMS addresses from which access to the MIB is allowed is specified. *ipv6-aclname*: IPv6 ACL name. The specified ACL is associated and the range of IPv6 NMS addresses from which access to the MIB is allowed is specified.
Command Mode	Global configuration mode
Usage Guide	Configure user information so that the NMS can communicate with the agent by using a valid user. For an SNMPv3 user, you can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (at present, only DES is available), and encryption password.

Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

Enabling the SNMP Attack Protection and Detection Function

Command	**snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }
Parameter Description	*times***:** Number of continuous failed attempts. **lock:** After continuous authentication fails, the source IP address is permanently forbidden to initiate authentication for access. The administrator needs to manually unlock the IP address. **lock-time** *minutes***:** After continuous authentication fails, the source IP address is forbidden to initiate authentication for access in a period of time. Beyond the period, the source IP address can be authenticated for access again. **unlock:** After continuous authentication fails, the source IP address is allowed to access the MIB continuously, which is equivalent to the fact that the SNMP attack protection and detection function is not configured.
Command	Global configuration mode

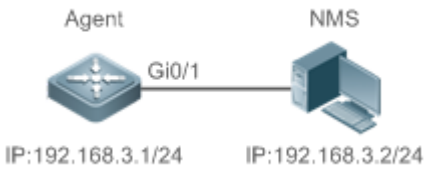
Mode	
Usage Guide	Configure the SNMP attack protection and detection function so that the corresponding measure can be taken after continuous authentication fails. The permanently forbidden source IP addresses can be authenticated for access again only after the administrator manually unlocks the IP addresses. The source IP address that are forbidden to access the MIB in a period of time can be authenticated for access again after the period expires or after the administrator manually unlocks the IP addresses.

Displaying the SNMP Status Information

Command	**show snmp** [**mib** | **user** | **view** | **group| host | locked-ip | process-mib-time**]
Parameter Description	**mib:** Displays information about the SNMP MIB supported in the system. **user:** Displays information about an SNMP user. **view:** Displays information about an SNMP view. **group:** Displays information about an SNMP user group. **host:** Displays information about user configuration. **locked-ip:** Source IP address that is locked after continuous authentication fails. **process-mib-time:** Displays the MIB node with the longest processing time.
Configuration mode	Privileged mode.
Usage Guide	N/A

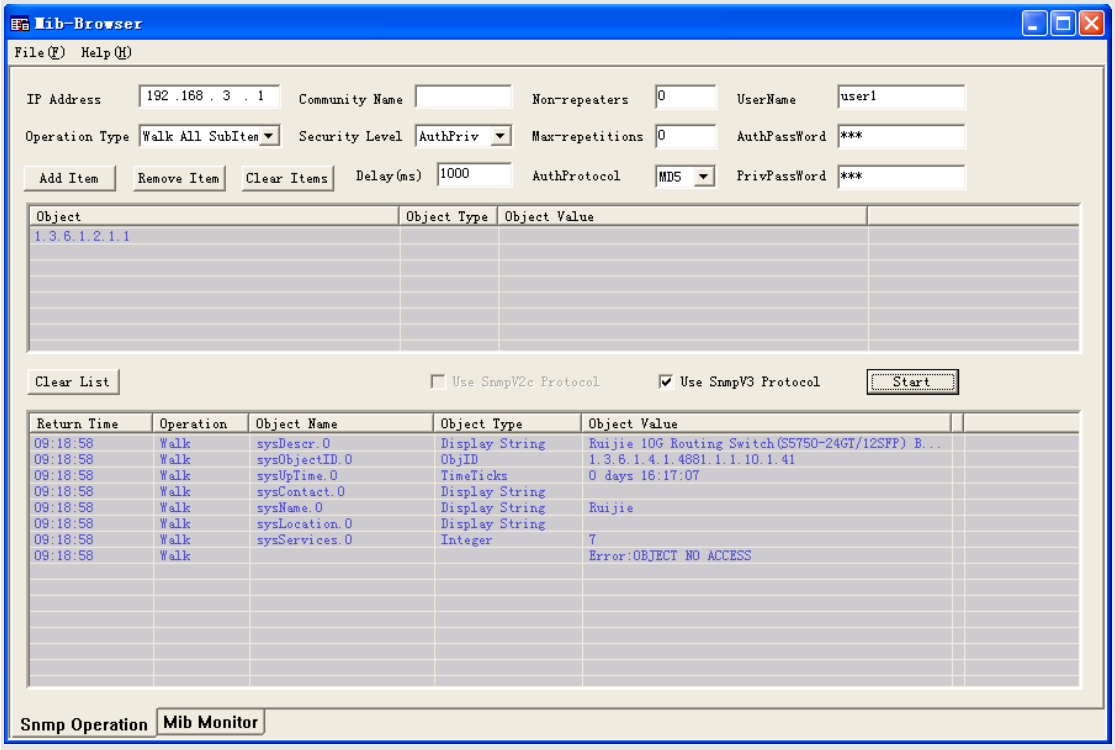
Configuration Example

Configuring SNMPv3 Configuration

Scenario Figure 5-5	 ● The NMS manages network devices (agents) based on the user authentication and encryption mode, for example, the NMS uses user1 as the user name, MD5 as the authentication mode, 123 as the authentication password, DES56 as the encryption algorithm, and 321 as the encryption password. ● Network devices can control the operation permission of users to access MIB objects. For example, the user named user1 can read MIB objects under the system node (1.3.6.1.2.1.1) and can only write MIB objects under the SysContact node (1.3.6.1.2.1.1.4.0). ● Network devices can actively send authentication and encryption messages to the NMS.
Configuration Steps	● Configure a MIB view and a MIB group. Create a MIB view “view1”, which includes the associated MIB object (1.3.6.1.2.1.1); then create a MIB view “view2”, which includes the associated MIB object (1.3.6.1.2.1.1.4.0). Create a group “g1”, select the version “v3”, set the security level to the

	authentication and encryption mode “priv”, and configure permissions to read the view “view1” and write the view “view2”. ● Configure an SNMP user. Create a user named “user1” under group “g1”, select “v3” as the version, and set the authentication mode to “md5”, authentication password to “123”, encryption mode to “DES56”, and encryption password to “321”. ● Configure the SNMP host address. Set the host address to 192.168.3.2, select “3” as the version, set the security level to the authentication and encryption mode “priv”, and associate the user name “user1”. Enable the agent to actively send a trap message to the NMS. ● Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2 Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 Ruijie(config)#snmp-server enable traps Ruijie(config)#interface gigabitEthernet 0/1 Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 Ruijie(config-if-gigabitEthernet 0/1)#exit
Verification	1. Run the **show running-config** command to display configuration information of the device. 2. Run the **show snmp user** command to display the SNMP user. 3. Run the **show snmp view** command to display the SNMP view. 4. Run the **show snmp group** command to display the SNMP group. 5. Run the **show snmp host** command to display the host information configured by the user. 6. Install MIB-Browser.
Agent	Ruijie# show running-config ! interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 ! snmp-server view view1 1.3.6.1.2.1.1 include snmp-server view view2 1.3.6.1.2.1.1.4.0 include snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56 D5CEC4884360373ABBF30AB170E42D03 snmp-server group g1 v3 priv read view1 write view2 snmp-server host 192.168.3.2 traps version 3 priv user1 snmp-server enable traps
	Ruijie# show snmp user User name: user1 Engine ID: 800013110300d0f8221120

	storage-type: permanent active Security level: auth priv Auth protocol: MD5 Priv protocol: DES Group-name: g1
	Ruijie#show snmp view view1(include) 1.3.6.1.2.1.1 view2(include) 1.3.6.1.2.1.1.4.0 default(include) 1.3.6.1
	Ruijie# show snmp group groupname: g1 securityModel: v3 securityLevel:authPriv readview: view1 writeview: view2 notifyview:
	Ruijie#show snmp host Notification host: 192.168.3.2 udp-port: 162 type: trap user: user1 security model: v3 authPriv
	Install MIB-Browser, enter IP address 192.168.3.1 in **IP Address** and **user1** in **UserName**, select **AuthPriv** for **Security Level**, enter **123** in **AuthPassWord**, select **MD5** for **AuthProtocol**, and enter **321** in **PrivPassWord**. Click **Add Item** and select a management unit for which the MIB needs to be queried, for example, **System** in the following **Figure**. Click **Start**. The MIB is queried for network devices. The lowest pane in the following figure shows query results.



Common Errors

-

5.4.2 Enabling the Trap Function

Configuration Effect

Enable the agent to actively send a trap message to the NMS.

Notes

N/A

Configuration Steps

Configuring the SNMP Host Address

- Optional
- Configure the host address of the NMS when the agent is required to actively send messages.

Enabling the Agent to Actively Send a Trap Message to the NMS

- Optional
- Configure this item on the agent when the agent is required to actively send a trap message to the NMS.

Enabling the Function of Sending a Link Trap Message on an Interface

- Optional
- Configure this item on the agent when a link trap message needs to be sent on an interface.

Enabling the Function of Sending a System Reboot Trap Message

- Optional
- Configure this item on the agent when the RGOS system is required to send a trap message to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

- Optional
- Configure this item on the agent when it is required to permanently use a local IP address as the source SNMP address to facilitate management.

Enabling a Trap Message to Carry Private Fields when the Message Is Sent

- Optional
- Configure this item on the agent when private fields need to be carried in a trap message.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the NMS Host Address

Command	**snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* }] [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]
Parameter Description	*host-addr*: Address of the SNMP host. *ipv6-addr*: (IPv6) address of the SNMP host. **traps | informs:** Configures the host to send a trap message or an inform message. **version:** SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv:** Sets the security level of V3 users. *community-string*: Community string or user name (V3). *port-num*: Configures the port ID of the SNMP host. *notification-type*: Type of trap messages that are actively sent, for example, snmp. If no trap type is specified, all trap messages are sent.
Command Mode	Global configuration mode
Usage Guide	This command is used with the **snmp-server enable traps** command to actively send trap messages to the NMS.

	You can configure different SNMP hosts to receive trap messages. A host can support different traps, and ports. If the same host is configured, the last configuration is combined with the previous configurations, that is, to send different trap messages to the same host, configure one type of trap messages each time. These configurations are finally combined.

Enabling the Agent to Actively Send a Trap Message to the NMS

Command	**snmp-server enable traps** [*notification-type*]
Parameter Description	*notification-type*: Enables trap notification for the corresponding events, including the following types: snmp: Enables trap notification for SNMP events. bridge: Enables trap notification for bridge events. mac-notification: Enables trap notification for MAC events. ospf: Enables trap notification for OSPF events. urpf: Enables trap notification for URPF events. vrrp: Enables trap notification for VRRP events. web-auth: Enables trap notification for Web authentication events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be actively sent.

Enabling the Function of Sending a Link Trap Message on an Interface

Command	**snmp trap link-status**
Parameter Description	**-**
Configuration mode	Interface configuration mode
Usage Guide	For interfaces (Ethernet interface, AP interface, and SVI interface), when this function is enabled, the SNMP sends a Link Trap message if the link status on the interfaces changes. Otherwise, the SNMP does not send the message.

Enabling the Function of Sending a System Reboot Trap Message

Command	**snmp-server system-shutdown**
Parameter Description	-
Configuration mode	Global configuration mode
Usage Guide	When the function of notification upon SNMP system reboot is enabled, a trap message is sent to the NMS to notify system reboot before reloading or reboot of the device.

Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*

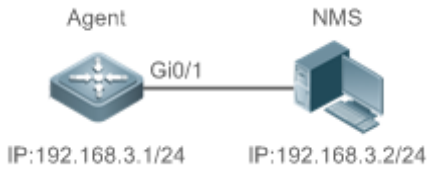
Parameter Description	*interface*: Used as the interface for the SNMP source address.
Configuration mode	Global configuration mode
Usage Guide	By default, the IP address of the interface where SNMP packets are sent is used as the source address. To facilitate management and identification, this command can be run to permanently use one local IP address as the source SNMP address.

Enabling a Trap message to Carry Private Fields when the Message Is Sent

Command	**snmp-server trap-format private**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to enable a trap message to carry private fields when the message is sent. At present, supported private fields include the alarm generation time. For the specific data types and data ranges of the fields, see RUIJIE-TRAP-FORMAT-MIB.mib.

Configuration Example

Enabling the Trap Function

Scenario Figure 5-6	 ● The NMS manages network devices (agents) based on the community authentication mode, and network devices can actively send messages to the NMS.
Configuration Steps	1. Perform configuration to enable the agent to actively send messages to the NMS. Set the SNMP host address to 192.168.3.2, the message format to Version2c, and the authentication name to user1. Enable the agent to actively send trap messages. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	`Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1` `Ruijie(config)#snmp-server enable traps` `Ruijie(config)#interface gigabitEthernet 0/1` `Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0` `Ruijie(config-if-gigabitEthernet 0/1)#exit`
Verification	● Run the **show running-config** command to display configuration information of the device. ● Run the **show snmp** command to display the SNMP status.

Agent	Ruijie# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location fuzhou snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact ruijie.com.cn snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Ruijie#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled

Common Errors

N/A

5.4.3 Shielding the Agent Function

Configuration Effect

Shield the agent function when the agent service is not required.

Notes

- Run the **no snmp-server** command to shield the SNMP agent function when the agent service is not required.
- Different from the shielding command, after the **no enable service snmp-agent** command is run, all SNMP services are directly disabled (that is, the SNMP agent function is disabled, no packet is received, and no response packet or trap packet is sent), but configuration information of the agent is not shielded.

Configuration Steps

Shielding the SNMP Agent Function for the Device

- Optional
- To shield the configuration of all SNMP agent services, use this configuration.

Disabling the SNMP Agent Function for the Device

- Optional
- To directly disable all services, use this configuration.

Verification

Run the **show services** command to check whether SNMP services are enabled or disabled.

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Shielding the SNMP Agent Function for the Device

Command	**no snmp-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run at the same time so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent

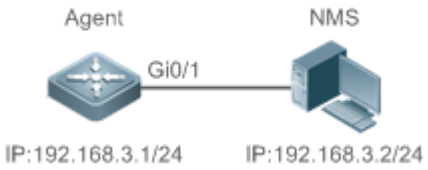
	configurations are not shielded.

Disabling the SNMP Agent Function for the Device

Command	**no enable service snmp-agent**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

Enabling the SNMP Service

Scenario Figure 5-7	 After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.
Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	`Ruijie(config)#enable service snmp-agent`
Verification	1. Run the **show services** command to check whether the SNMP service is enabled or disabled.
Agent	`Ruijie#show service` `web-server : disabled` `web-server(https): disabled` `snmp-agent : enabled` `ssh-server : disabled` `telnet-server : enabled`

Common Errors

N/A

5.4.4 Setting SNMP Control Parameters

Configuration Effect

Set basic parameters of the SNMP agent, including the device contact mode, device location, serial number, and parameters for sending a trap message. By accessing the parameters, the NMS can obtain the contact person of the device and physical location of the device.

Notes

N/A

Configuration Steps

Setting the System Contact Mode

- Optional
- When the contact mode of the system needs to be modified, configure this item on the agent.

Setting the System Location

- Optional
- When the system location needs to be modified, configure this item on the agent.

Setting the System Serial Number

- Optional
- When the system serial number needs to be modified, configure this item on the agent.

Setting NE Information about the Device

- Optional
- When the NE code needs to be modified, configure this item on the agent.

Setting the Maximum Packet Length of the SNMP Agent

- Optional
- When the maximum packet length of the SNMP agent needs to be modified, configure this item on the agent.

Setting the UDP Port ID of the SNMP Service

- Optional
- When the UDP port ID of the SNMP service needs to be modified, configure this item on the agent.

Setting the Queue Length of Trap Messages

- Optional
- When the size of the message queue needs to be adjusted to control the message sending speed, configure this item on the agent.

Setting the Interval for Sending a Trap Message

- Optional

- When the interval for sending a trap message needs to be modified, configure this item on the agent.

Configuring SNMP Flow Control

- Optional
- If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Verification

Run the **show snmp** command to display the SNMP status.

Run the **show running-config** command to display configuration information of the device.

Related Commands

Setting the System Contact Mode

Command	**snmp-server contact** *text*
Parameter Description	*text*: String that describes the system contact mode.
Command Mode	Global configuration mode
Usage Guide	N/A

Setting the System Location

Command	**snmp-server location** *text*
Parameter Description	*text*: String that describes system information.
Configuration mode	Global configuration mode
Usage Guide	N/A

Setting the System Serial Number

Command	**snmp-server chassis-id** *text*
Parameter Description	*text*: Text of the system serial number, which may be digits or characters.
Configuration mode	Global configuration mode
Usage Guide	In general, the device serial number is used as the SNMP serial number to facilitate identification of the device.

Setting NE Information about the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Text that is used to set the device NE code. The text is a string that consists of 1 to 255 characters that are case-sensitive and may include spaces.
Configuration mode	Global mode.
Usage Guide	Set the NE code of the device.

Setting the Maximum Packet Length of the SNMP Agent

Command	**snmp-server packetsize** *byte-count*
Parameter Description	*byte-count*: Packet size, ranging from 484 bytes to 17,876 bytes.
Configuration mode	Global mode.
Usage Guide	N/A

Setting the UDP Port ID of the SNMP Service

Command	**snmp-server udp-port** *port-num*
Parameter Description	*port-num*: Specifies the UDP port ID of the SNMP service, that is, the ID of the protocol port that receives SNMP packets.
Configuration mode	Global mode.
Usage Guide	Specify the protocol port ID for receiving SNMP packets.

Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Queue length, ranging from 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the size of the message queue to control the message sending speed.

Setting the Interval for Sending a Trap Message

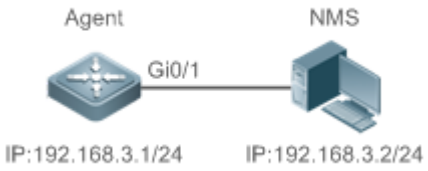
Command	**snmp-server trap-timeout** *seconds*
Parameter Description	*seconds*: Interval (unit: second). The value range is 1 to 1,000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

Configuring SNMP Flow Control

Command	**snmp-server flow-control pps** [*count*]
Parameter Description	*count*: Number of SNMP request packets processed per second. The value range is 50 to 65,535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in high CPU usage for SNMP tasks, configure SNMP flow control to limit the number of request packets processed per second in each SNMP task, so as to control the CPU usage for SNMP tasks.

Configuration Example

Setting SNMP Control Parameters

Scenario	
Figure 5-8	 ● The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.
Configuration Steps	1. Set SNMP agent parameters. Set the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of the Gi0/1 interface to 192.168.3.1/24.
Agent	`Ruijie(config)#snmp-server location fuzhou` `Ruijie(config)#snmp-server contact ruijie.com.cn` `Ruijie(config)#snmp-server chassis-id 1234567890` `Ruijie(config)#interface gigabitEthernet 0/1` `Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0` `Ruijie(config-if-gigabitEthernet 0/1)#exit`
Verification	1. Check the configuration information of the device. 2. Check the SNMP view and group information.
Agent	`Ruijie# show running-config` `ip access-list standard a1` `10 permit host 192.168.3.2` `interface gigabitEthernet 0/1` `no ip proxy-arp` `ip address 192.168.3.1 255.255.255.0` `snmp-server view v1 1.3.6.1.2.1.1 include` `snmp-server location fuzhou`

	snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact ruijie.com.cn snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	Ruijie#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 Ruijie#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview: groupname: user1 securityModel: v2c securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview:

Common Errors

N/A

5.4.5 Configuring SNMP MIB Cache Function

Configuration Effect

Enable the SNMP MIB cache function to increase the speed of obtaining MIB data by the NMS. This function enables the master device to collect MIB variables on the slave/backup device in advance and cache the collected MIB variables. In this way, the NMS can directly read the cached MIB variables from the master device, avoid accessing the slave/backup device and reducing the consumed time.

Notes

- The SNMP MIB cache function applies only to MIB nodes with specific table variables. To configure this function, only the OID of the root node of the MIB table variables needs to be configured.
- After the cache function is enabled, the cache is updated periodically, and the MIB data is not collected in real time. An excessively short cache update interval may cause frequent cache update operations in the system, which consumes many CPU resources; on the contrary, an excessively long cache update interval may delay MIB data updates, which fails to reflect the system status in real time. Therefore, the cache update interval needs to be adjusted according to the real-time performance of the MIB nodes and the CPU resources.

Configuration Steps

Configuring Global SNMP MIB Cache Function

- Optional.
- The SNMP MIB cache function is disabled by default. You can enable the MIB cache function globally.

Configuring Global SNMP MIB Cache Update Interval

- Optional.
- The global SNMP MIB cache update interval is 300 seconds by default. You can configure the global cache update interval.

Enabling Cache Function on Node with Specified OID and Configuring Cache Update Interval of This Node

- Optional.
- The cache function is disabled on all MIB nodes by default. You can enable the MIB cache function on a specified MIB node.

Verification

Run the **show running-config** command to display the configuration information of the device.

Related Commands

Configuring Global SNMP MIB Cache Function.

Command	**snmp-server cache enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	

Configuring Global SNMP MIB Cache Update Interval

Command	**snmp-server cache update-timer** *seconds*
Parameter Description	*seconds*: Specifies the global SNMP MIB cache update interval in seconds. The value ranges from 60 to 3,600.
Configuration Mode	Global configuration mode
Usage Guide	

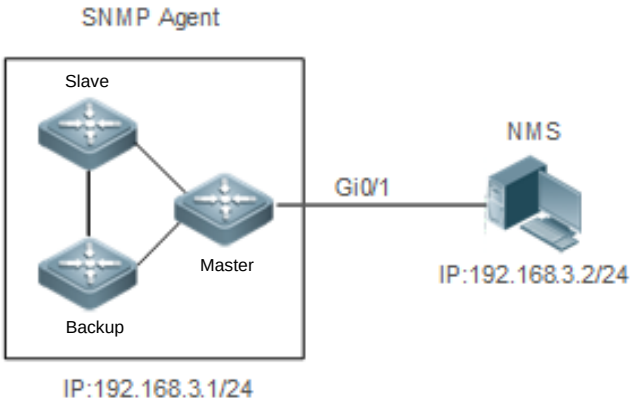
Enabling Cache Function on Node with Specified OID and Configuring Cache Update Interval of This Node

Command	**snmp-server cache oid** *oid-string* [**update-timer** *seconds*]
Parameter	*oid-string*: Specifies the OID of the MIB node.

Description	*seconds*: Specifies the cache update interval in seconds. The value ranges from 60 to 3,600.
Configuration Mode	Global configuration mode
Usage Guide	The cache update interval of the MIB node, if not configured, is consistent with the global cache update interval

Configuration Example

Setting SNMP Control Parameters

Scenario Figure 5-9	 ● The NMS manages the SNMP agent based on the community authentication mode. The NMS can obtain the MIB node information of the SNMP agent, such as the connection statuses of the AP and STA.
Configuration Steps	1. Configure the global SNMP MIB cache function. 2. Configure the global SNMP MIB cache update interval. 3. Enable the cache function on a node with a specified OID.
Agent	`Ruijie(config)# snmp-server cache enable` `Ruijie(config)# snmp-server cache update-timer 600` `Ruijie(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1`
Verification	● Display the configuration information of the device.
Agent	`Ruijie# show running-config | include snmp` `snmp-server cache enable` `snmp-server cache update-timer 600` `snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1` `snmp-server enable traps` `snmp-server community public rw`

Common Errors

N/A

5.5 Monitoring

Clearing

Description	Command
Clears the list of source IP addresses that are locked after continuous authentication fails.	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

Displaying

Description	Command
Displays the SNMP status.	**show snmp** [**mib** | **user** | **view** | **group**| **host**]

6 Configuring HTTP Service

6.1 Overview

Hypertext Transfer Protocol (HTTP) is used to transmit Web page information on the Internet. It is at the application layer of the TCP/IP protocol stack. The transport layer adopts connection-oriented Transmission Control Protocol (TCP).

Hypertext Transfer Protocol Secure (HTTPS) is an HTTP supporting the Secure Sockets Layer (SSL) protocol. HTTPS is mainly used to create a secure channel on an insecure network, ensure that information can hardly be intercepted, and provide certain reasonable protection against main-in-the-middle attacks. At present, HTTPS is widely used for secure and sensitive communication on the Internet, for example, electronic transactions.

Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: Hypertext Transfer Protocol Over TLS -- HTTPS

6.2 Applications

Application	Description
HTTP Application Service	Users manage devices based on Web.

6.2.1 HTTP Application Service

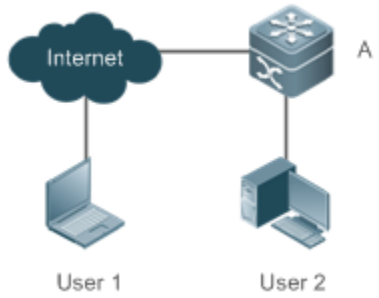
Scenario

After the HTTP service is enabled, users can access the Web management page after passing authentication by only entering **http://IP address of a device** in the browser of a PC. On the Web page, users you can monitor the device status, configure devices, upload and download files.

Take the following figure as an example to describe Web management.

- Users can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the Web server.
- According to actual conditions, users can choose to enable the HTTPS or HTTP service or enable the HTTPS and HTTP services at the same time.
- Users can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 6-1



Remarks	A is a Ruijie device. User 1 accesses the device through the Internet. User 2 accesses the device through a LAN.

Deployment

- When a device runs HTTP, users can access the device by entering **http://IP address of the device** in the browser of a PC.
- When a device runs HTTPS, users can access the device by entering **https://IP address of the device** in the browser of a PC.

6.3 Features

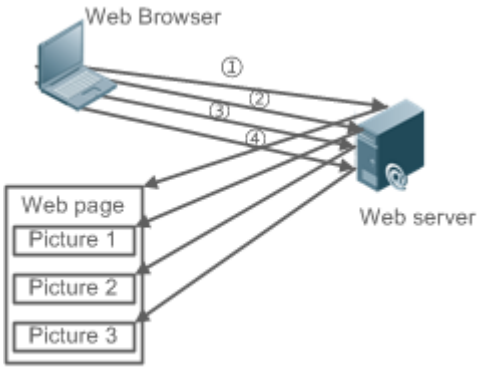
Basic Concepts

↘ HTTP Service

The HTTP service refers to transmission of Web page information on the Internet by using HTTP. HTTP/1.0 is currently an HTTP version that is the most widely used. As one Web server may receive thousands or even millions of access requests, HTTP/1.0 adopts the short connection mode to facilitate connection management. One TCP connection is established for each request. After a request is completed, the TCP connection is released. The server does not need to record or trace previous requests. Although HTTP/1.0 simplifies connection management, HTTP/1.0 introduces performance defects.

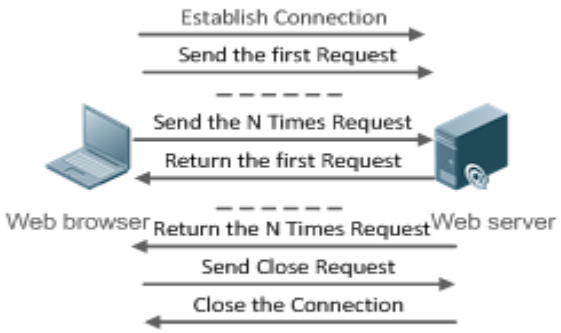
For example, a web page my need lots of pictures. However, the web page contains not real picture contents but URL connection addresses of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishing an independent connection and each connection is completely isolated. Establishing and releasing connections is a relatively troublesome process, which severely affects the performance of the client and server, as shown in the following figure:

Figure 6-2



HTTP/1.1 overcomes the defect. It supports persistent connection, that is, one connection can be used to transmit multiple requests and response messages. In this way, a client can send a second request without waiting for completion of the previous request. This reduces network delay and improves performance. See the following figure:

Figure 6-3



At present, Ruijie devices support both HTTP/1.0 and HTTP/1.1.

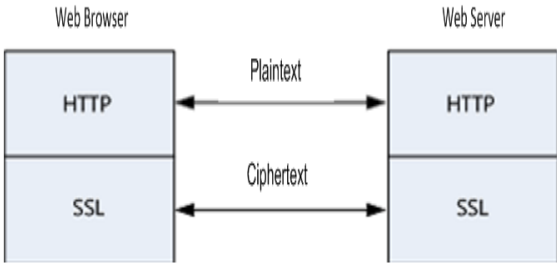
Which HTTP version will be used by a device is decided by the Web browser.

HTTPS Service

The HTTPS service adds the SSL based on the HTTP service. Its security basis is the SSL. To run HTTPS properly, a server must have a Public Key Infrastructure (PKI) certificate while a client may not necessarily need one. The SSL protocol provides the following services:

- Authenticating users and servers and ensuring that data is sent to the correct client and server.
- Encrypting data to prevent data from being stolen midway.
- Maintaining data integrity and ensuring that data is not changed during transmission.

Figure 6-4



HTTP Upgrade Service

HTTP upgrade includes local HTTP upgrade and remote HTTP upgrade.

- During a local upgrade, a device serves as an HTTP server. Users can log in to the device through a Web browser and upload upgrade files to the device to realize file upgrade on the device.
- During a remote upgrade, a device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Features

Feature	Description
HTTP Service	Users log in to devices through Web pages to configure and manage devices.
Local HTTP Upgrade Service	Upgrade files are uploaded to a device to realize file upgrade on the device.

6.3.1 HTTP Service

HTTP is a service provided for Web management. Users log in to devices through Web pages to configure and manage devices.

Working Principle

Web management covers Web clients and Web servers. Similarly, the HTTP service also adopts the client/server mode. The HTTP client is embedded in the Web browser of the Web management client. It can send HTTP packets and receive HTTP response packets. The Web server (namely HTTP server) is embedded in devices. The information exchange between the client and the server is as follows:

- A TCP connection is established between the client and the server. The default port ID of the HTTP service is 80 and the default port ID of the HTTPS service is 443.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request content includes obtaining a Web page, executing a CLI command, and uploading a file.

- After executing the request content, the server sends a response message to the client.

Related Configuration

Enabling the HTTP Service

By default, the HTTP service is disabled.

The **enable service web-server** command can be used to enable HTTP service functions, including the HTTP service and HTTPS service.

The HTTP service must be enabled so that users can log in to devices through Web pages to configure and manage devices.

Configuring HTTP Authentication Information

By default, the system creates the **admin** and the **guest** account. The accounts cannot be deleted and only the password of the account can be changed. The administrator account is the **admin** account, which corresponds to the level 0 permission. The **admin** account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The **guest** account corresponds to the level 2 permission. The **guest** account can only view the homepage. The new accounts that are added correspond to the level 1 permission.

The **webmaster level** command can be used to configure an authenticated user name and a password.

After this command is run, you need to enter the configured user name and password to log in to the Web page.

Configuring an HTTP Service Port

By default, the HTTP service port ID is 80.

The **http port** command can be used to configure an HTTP service port ID. The value range of the port ID is 80 and 1025 to 65535.

By configuring an HTTP service port ID, you can reduce the number of attacks initiated by illegal users on the HTTP service.

Configuring an HTTPS Service Port

By default, the HTTPS service port ID is 443.

The **http secure-port** command can be used to configure an HTTPS service port ID. The value range of the port ID is 443 and 1025 to 65535.

By configuring an HTTPS service port ID, you can reduce the number of attacks initiated by illegal users on the HTTPS service.

6.3.2 Local HTTP Upgrade Service

When a device serves as the HTTP server, users can log in to the device through a Web browser and upload upgrade files (including component package and Web package) to the device or directly upload files to the device through Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or Web package is uploaded through the local upgrade function provided by Web.
- After successfully receiving a file, the device checks the version for its validity.
- After the file check is successful, if the file is a Web package, perform the upgrade directly; if the file is a component package, decide whether to perform the upgrade in the browser by restarting the device.

Related Configuration

Updating a Web Package

Run the **upgrade web download** command to download a Web package from the TFTP server.

After the command is run, download a Web package from the TFTP server. After the package passes the validity check, directly use the Web package for upgrade without restarting the device.

You can also run the **upgrade web** command to directly upgrade a Web package stored locally.

Updating a Subsystem Component

By default, a device does not upgrade subsystem components uploaded through a browser or TFTP.
To upgrade a subsystem component, you must restart the device.

6.4 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	(Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring a Local HTTP Upgrade	(Mandatory) It is used to realize a local HTTP upgrade.	
	upgrade web	Upgrades a Web package stored on a device.
	upgrade web download	Automatically downloads a Web package from a server and automatically upgrades the package.

6.4.1 Configuring the HTTP Service

Configuration Effect

After the HTTP service is enabled on a device, users can log in to the Web management page after passing authentication and monitor the device status, configure devices, upload and download files.

Configuration Steps

Enabling the HTTP Service

- Mandatory
- If there is no special requirement, enable the HTTP service on Ruijie devices. Otherwise, the Web service is inaccessible.

Configuring HTTP Authentication Information

- By default, the user name **admin** and the password **admin** are configured.
- If there is no special requirement, you can log in to the Web page by using the default user name and directly update authentication information through the Web browser. If you always use the default account, security risks may exist because unauthorized personnel can obtain device configuration information once the IP address is disclosed.

Configuring an HTTP Service Port

- If an HTTP service port needs to be changed, the HTTP service port must be configured.
- If there is no special requirement, the default HTTP service port 80 can be used for access.

Configuring an HTTPS Service Port

- If an HTTPS service port needs to be changed, the HTTPS service port must be configured.
- If there is no special requirement, the default HTTPS service port 443 can be used for access.

Verification

- Enter **http://IP address of the device: service port** to check whether the browser skips to the authentication page.
- Enter **https://IP address of the device: service port** to check whether the browser skips to the authentication page.

Related Commands

Enabling the HTTP Service

Command	**enable service web-server** [**http** | **https** | **all**]
Parameter Description	**http** | **https** | **all**: Enables the corresponding service. **http** indicates enabling the HTTP service, **https** indicates enabling the HTTPS service, and **all** indicates enabling the HTTP and HTTPS services at the same time. By default, the HTTP and HTTPS services are enabled at the same time.
Command Mode	Global configuration mode.
Usage Guide	If no key word or **all** is put at the end of the command when the command is run, the HTTP and HTTPS services are enabled at the same time. If the key word **http** is put at the end of the command, only the HTTP service is enabled; if the key word **https** is put at the end of the command, only the HTTPS service is enabled. The **no enable service web-server** or **default enable service web-server** command is used to disable the

	corresponding HTTP service. If no key word is put at the end of the **no enable service web-server** or **default enable service web-server** command, the HTTP and HTTPS services are disabled.

Configuring HTTP Authentication Information.

Command	**webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }
Parameter Description	*privilege-level*: Permission level bound to a user. *name*: User name. *password*: User password. **0 | 7**: Password encryption type. 0: no encryption; 7: simple encryption. The default value is **0**. *encrypted-password*: Password text.
Command Mode	Global configuration mode.
Usage Guide	When the HTTP server is used, you need to be authenticated before logging in to the Web page. The **webmaster level** command is used to configure a user name and a password for logging in to the Web page. Run the **no webmaster level** *privilege-level* command to delete all user names and passwords of the specified permission level. Run the **no webmaster level** *privilege-level* **username** *name* command to delete the specified user name and password. User names and passwords involve three permission levels: Up to 10 user names and passwords can be configured for each permission level. By default, the system creates the **admin** account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the **admin** account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The new accounts that are added correspond to the level 1 permission.

Configuring an HTTP Service Port

Command	**http port** *port-number*
Parameter Description	*port-number*: Configures an HTTP service port. The value range is 80 and 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTP service port.

Configuring an HTTPS Service Port

Command	**http secure-port** *port-number*
Parameter Description	*port-number*: Configures an HTTPS service port. The value range is 443 and 1025 to 65535.

Command Mode	Global configuration mode.
Usage Guide	Run the command to set an HTTPS service port.

Configuration Example

Managing one Ruijie Device by Using Web and Logging in to the Device through a Web Browser to Configure Related Functions

- Log in to the device by using the **admin** account configured by default.
- To improve security, the Web browser is required to support both HTTP and HTTPS for access.
- The user is required to configure an HTTP service port to reduce the number of attacks initiated by illegal users on HTTP.

Scenario Figure 6-5	
Configuration Steps	● Enable the HTTP and HTTPS services at the same time. ● Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.
A	A#configure terminal A(config)# enable service web-server A(config)# http port 8080 A(config)# http secure-port 4430
Verification	Check HTTP configurations.
A	A# show web-server status http server status: enabled http server port: 8080 https server status:enabled https server port: 4430

Common Errors

- If the HTTP service port is not the default port 80 or 443, you must enter a specific configured service port in the browser. Otherwise, you cannot access devices on the Web client.

6.4.2 Configuring a Local HTTP Upgrade

Configuration Effect

Perform an HTTP upgrade through the browser or the **upgrade web** command.

Notes

- So long as a Web package is uploaded successfully and passes the version check, the device directly performs an upgrade based on the latest Web package.
- The **upgrade web download** command is used to automatically download files from the TFTP server and automatically perform an upgrade.
- The **upgrade web** command is used to automatically upgrade the Web package in the local file system.

Configuration Steps

N/A

Verification

- Access and view the latest Web page through the browser.

Related Commands

Downloading a Web Package from the TFTP Server

Command	**upgrade web download tftp:** */path*
Parameter Description	*tftp:* Connects the FTFP server through a common data port and downloads a Web package. *path*: Path of a Web package on the TFTP server.
Command Mode	Privileged mode
Usage Guide	This command is used to download a Web package from the TFTP server and automatically perform an upgrade.

Upgrading a Web Package Stored on a Local Device

Command	**upgrade web** *uri*
Parameter Description	*uri*: Local path for storing a Web package.
Command Mode	Privileged mode
Usage Guide	This command is used to upgrade a Web package stored on a device and automatically perform an upgrade.

Configuration Example

Obtaining the Latest Web Package from the Official Website and Running the Web Package

Scenario **Figure 6-6**	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Log in to the device through Web and upload the latest Web package to the device.
A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# exit A(config)# enable service web-server
	On a PC, use the local upgrade function on the Web page to upload a Web package for upgrade.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Upgrading a Web Package by Running the upgrade web download Command

Scenario **Figure 6-7**	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#upgrade web download tftp:// 10.10.10.13/web.upd Press Ctrl+C to quit !!!!!!!! download 3896704 bytes

	Begin to upgrade the web package... Web package upgrade successfully.
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Upgrading a Web Package by Running the upgrade web Command

Scenario **Figure 6-8**	
Configuration Steps	● Connect to a local PC whose IP address is 10.10.10.13 and assign an IP address 10.10.10.131 in the same network segment to the device. ● Start the TFTP server.
A	A#configure terminal A(config)# vlan 1 A(config-vlan)# exit A(config)# interface vlan 1 A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0 A(config-VLAN 1)# end A#copy tftp://10.10.10.13/web.upd flash:/web.upd Press Ctrl+C to quit !!!!!!!! Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared Flushing data to flash:/web.upd... Flush data done A #upgrade web flash:/web.upd Web package upgrade successfully. A #
Verification	On the PC, log in to the device through Web again and check whether the latest Web page is displayed.

Common Errors

- Access to the web page through the browser shows that the web page is not updated based on the latest Web package. This is possibly because the local browser has a cache. Clear the cache of the local browser and access the Web page again.

6.5 Monitoring

Displaying

Description	Command
Displays the configuration and status of the Web service.	**show web-server status**

7 Configuring Syslog

7.1 Overview

Status changes (such as link up and down) or abnormal events may occur anytime. Ruijie products provide the syslog mechanism to automatically generate messages (log packets) in fixed format upon status changes or occurrence of events. These messages are displayed on the related windows such as the Console or monitoring terminal, recorded on media such as the memory buffer or log files, or sent to a group of log servers on the network so that the administrator can analyze network performance and identify faults based on these log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity level so that the administrator can conveniently read and manage log packets.

Protocols and Standards

- RFC3164: The BSD syslog Protocol
- RFC5424: The_Syslog_Protocol

7.2 Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the Console.
Sending Syslogs to the Log Server	Monitor syslogs through the server.

7.2.1 Sending Syslogs to the Console

Scenario

Send syslogs to the Console to facilitate the administrator to monitor the performance of the system. The requirements are as follows:

1. Send logs of Level 6 or higher to the Console.
2. Send logs of only the ARP and IP modules to the Console.

Figure 7-1 shows the network topology.

Figure 7-1 Network topology

Deployment

Configure the device as follows:

1. Set the level of logs that can be sent to the Console to informational (Level 6).
2. Set the filtering direction of logs to terminal.
3. Set log filtering mode of logs to contains-only.
4. Set the filtering rule of logs to single-match. The module name contains only ARP or IP.

7.2.2 Sending Syslogs to the Log Server

Scenario

Send syslogs to the log server to facilitate the administrator to monitor the logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server 10.1.1.1.
2. Send logs of Level 7 or higher to the log server.
3. Send syslogs from the source interface Loopback 0 to the log server.

Figure 7-2 shows the network topology.

Figure 7-2 Network topology

Deployment

Configure the device as follows:

1. Set the IPv4 address of the server to 10.1.1.1.
2. Set the level of logs that can be sent to the log server to debugging (Level 7).
3. Set the source interface of logs sent to the log server to Loopback 0.

7.3 Features

Basic Concepts

Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

Levels of Syslogs

Eight severity levels of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These levels correspond to eight numerical values from 0 to 7. A smaller value indicates a higher level.

Only logs with a level equaling to or higher than the specified level can be output. For example, if the level of logs is set to informational (Level 6), logs of Level 6 or higher will be output.

The following table describes the log levels.

Level	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that the measures must be taken immediately.
critical	2	Indicates a critical condition.
errors	3	Indicates an error.
warnings	4	Indicates a warning.
notifications	5	Indicates a notification message that requires attention.
informational	6	Indicates an informational message.
debugging	7	Indicates a debugging message.

Output Direction of Syslogs

Output directions of syslogs include Console, monitor, server, buffer, and file. The default level and type of logs vary with the output direction. You can customize filtering rules for different output directions.

The following table describes output directions of syslogs.

Output Direction	Description	Default Output Level	Description
Console	Console	Debugging (Level 7)	Logs and debugging information are output.
monitor	Monitoring terminal	Debugging (Level 7)	Logs and debugging information are output.
server	Log server	Informational (Level 6)	Logs and debugging information are output.
buffer	Log buffer	Debugging (Level 7)	Logs and debugging information are output. The log buffer is used to store syslogs.
file	Log file	Informational (Level 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.

RFC3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If the output direction is the Console, monitor, buffer, or file, the syslog format is as follows:

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

- If the output direction is the log server, the syslog format is as follows:

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

For example, if you exit configuration mode, the following log is displayed on the log server:

```
<189>001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

The following describes each field in the log in details:

7. Priority

This field is valid only when logs are sent to the log server.

The priority is calculated using the following formula: Facility x 8 + Level Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. The default facility value is local7 (23). The following table lists the value range of the facility.

Numerical Code	Facility Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogs
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon
10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

8. Sequence Number

The sequence number of a syslog is a 6-digit integer, and increases sequentially. By default, the sequence number is not displayed. You can run a command to display or hide this field.

9. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Ruijie devices support two syslog timestamp formats: datetime and uptime.

If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.

The two timestamp formats are described as follows:

- Datetime format

The datetime format is as follows:

```
Mmm dd yyyy hh:mm:ss.msec
```

The following table describes each parameter of the datetime.

Timestamp Parameter	Parameter Name	Description
Mmm	Month	Mmm refers to abbreviation of the current month. The 12 months in a year are written as Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
dd	Day	dd indicates the current date.
yyyy	Year	yyyy indicates the current year, and is not displayed by default.
hh	Hour	hh indicates the current hour.
mm	Minute	mm indicates the current minute.
ss	Second	ss indicates the current second.
msec	Millisecond	msec indicates the current millisecond.

By default, the datetime timestamp displayed in the syslog does not contain the year and millisecond. You can run a command to display or hide the year and millisecond of the datetime timestamp.

- Uptime format

The uptime format is as follows:

```
dd:hh:mm:ss
```

The timestamp string indicates the accumulated days, hours, minutes, and seconds since the system is started.

10. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log. By default, this field is not displayed. You can run a command to display or hide this field.

11. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

12. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

13. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which may include upper-case letters, digits, or underscore. The mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

14. Content

This field indicates the detailed content of the syslog.

RFC5424 Log Format

The syslog format in the output direction is as follows:

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

For example, if you exit configuration mode, the following log is displayed on the Console:

```
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
```

The following describes each field in the log in details:

15. Priority

The priority is calculated using the following formula: Facility x 8 + Level. Level indicates the numerical code of the log level and Facility indicates the numerical code of the facility. When the RFC5424 format is enabled, the default value of the facility field is local0 (16).

16. Version

According to RFC5424, the version is always 1.

17. Timestamp

The timestamp records the time when a syslog is generated so that you can display and check the system event conveniently. Ruijie devices use the following uniformed timestamp format when the RFC5424 logging function is enabled:

```
YYYY-MM-DDTHH:MM:SS.SECFRACZ
```

The following table describes each parameter of the timestamp.

Timestamp Parameter	Description	Remark
YYYY	Year	YYYY indicates the current year.
MM	Month	MM indicates the current month.
DD	Day	DD indicates the current date.
T	Separator	The date must end with "T".
HH	Hour	HH indicates the current hour.
MM	Minute	MM indicates the current minute.
SS	Second	SS indicates the current second.
SECFRAC	Millisecond	SECFRAC indicates the current millisecond (1–6 digits).
Z	End mark	The time must end with "Z".

18. Sysname

This field indicates the name of the device that generates the log so that the log server can identify the host that sends the log.

19. Module

This field indicates the name of the module that generates the log. The module name is an upper-case string of 2 to 20 characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in the log-type information, and optional in the debug-type information.

20. Level

Eight syslog levels from 0 to 7 are defined. The level of syslogs generated by each module is fixed and cannot be modified.

21. Mnemonic

This field indicates the brief information about the log. The mnemonic is an upper-case string of 4 to 32 characters, which contain upper-case letters, digits, or underscores. The Mnemonic field is mandatory in the log-type information, and optional in the debug-type information.

22. Structured-Data

Structured-data introduced in RFC5424 is parsed as a whole string containing parameter information. Each log may contain 0 or multiple parameters. If a parameter is null, replace this parameter with a placeholder (-). The format of this field is as follows:

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

The following table describes each parameter of the structured-data field.

Parameter in structured-data	Description	Remarks
SD_ID	Parameter information name	The parameter information name is capitalized, and must be unique in a log.
@	Separator	"@enterpriseID" is added only to the customized parameter information, not to the parameter information defined in RFC5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). Ruijie Networks' enterprise ID is 4881. You can query the enterprise ID on the official website of IANA. `http://www.iana.org/assignments/enterprise-numbers`
PARAM-NAME	Parameter name	The parameter name is capitalized, and must be unique in the structured-data of a log.
PARAM-VALUE	Parameter value	The parameter value must be enclosed in double quotation marks. Values of the IP address or MAC address must be capitalized, and other types of values are capitalized as required.

23. description

This field indicates the content of the syslog.

Overview

Feature	Description
Logging	Enable or disable the system logging functions.
Syslog Format	Configure the syslog format.
Logging Direction	Configure the parameters to send syslogs in different directions.
Syslog Filtering	Configure parameters of the syslog filtering function.
Featured Logging	Configure parameters of the featured logging function.
Syslog Monitoring	Configure parameters of the syslog monitoring function.

7.3.1 Logging

Enable or disable the logging and log statistics functions.

Related Configuration

Enable Logging

By default, logging is enabled.

Run the **logging on** command to enable logging in global configuration mode. After logging is enabled, logs generated by the system are sent in various directions for the administrator to monitor the performance of the system.

Enabling Log Statistics

By default, log statistics is disabled.

Run the **logging count** command to enable log statistics in global configuration mode. After log statistics is enabled, the system records the number of times a log is generated and the last time when the log is generated.

7.3.2 Syslog Format

Configure the syslog format, including the RFC5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

Enabling the RFC5424 Log Format

By default, the RFC5424 log format is disabled.

After the new format (RFC5424 log format) is enabled, the **service sequence-numbers, service sysname, service timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC3164 log format) lose effect and are hidden.

After the old format (RFC3164 log format) is enabled, the **logging delay-send, logging policy**, and **logging statistic** commands that are applicable only to the RFC5424 log format lose effect and are hidden.

After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuring the Timestamp Format

By default, the syslog uses the datetime timestamp format, and the timestamp does not contain the year and millisecond.

Run the **service timestamps** command in global configuration mode to use the datetime timestamp format that contains the year and millisecond in the syslog, or change the datetime format to the uptime format.

Adding Sysname to the Syslog

By default, the syslog does not contain sysname.

Run the **service sysname** command in global configuration mode to add sysname to the syslog.

Adding the Sequence Number to the Syslog

By default, the syslog does not contain the sequence number.

Run the **service sequence-numbers** command in global configuration mode to add the sequence number to the syslog.

Enabling the Standard Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service standard-syslog** command in global configuration mode to enable the standard log format and logs are displayed in the following format:

```
timestamp %module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Log Format

By default, logs are displayed in the following format:

```
*timestamp: %module-level-mnemonic: content
```

Run the **service private-syslog** command in global configuration mode to enable the private log format and logs are displayed in the following format:

```
timestamp module-level-mnemonic: content
```

Compared with the default log format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing at the end of the module name in the private log format.

7.3.3 Logging Direction

Configure parameters for sending syslogs in different directions, including the Console, monitor terminal, buffer, the log server, and log files.

Related Configuration

Configuring the Log Rate Limit

By default, no log rate limit is configured.

Run the **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]] command in global configuration mode to configure the log rate limit.

Configuring the Level of Logs Sent to the Console

By default, the level of logs sent to the Console is debugging (Level 7).

Run the **logging console** [*level*] command in global configuration mode to configure the level of logs that can be sent to the Console.

Sending Logs to the Monitor Terminal

By default, it is not allowed to send logs to the monitor terminal.

Run the **terminal monitor** command in the privileged EXEC mode to send logs to the monitor terminal.

Configuring the Level of Logs Sent to the Monitor Terminal

By default, the level of logs sent to the monitor terminal is debugging (Level 7).

Run the **logging monitor** [*level*] command in global configuration mode to configure the level of logs that can be sent to the monitor terminal.

Writing Logs into the Memory Buffer

By default, logs are written into the memory buffer, and the default level of logs is debugging (Level 7).

Run the **logging buffered** [*buffer-size*] [*level*] command in global configuration mode to configure parameters for writing logs into the memory buffer, including the buffer size and log level.

Sending Logs to the Log Server

By default, logs are not sent to the log server.

Run the **logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*] command in global configuration mode to send logs to a specified log server.

Configuring the Level of Logs Sent to the Log Server

By default, the level of logs sent to the log server is informational (Level 6).

Run the **logging trap** [*level*] command in global configuration mode to configure the level of logs that can be sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

If the RFC5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 log format is enabled, the facility value of logs sent to the log server is local0 (16) by default.

Run the **logging facility** *facility-type* command in global configuration mode to configure the facility value of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

By default, the source address of logs sent to the log server is the IP address of the interface sending logs.

Run the **logging source** [**interface**] *interface-type interface-number* command to configure the source interface of logs. If this source interface is not configured, or the IP address is not configured for this source interface, the source address of logs is the IP address of the interface sending logs.

Run the **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address of logs. If this IP address is not configured on the device, the source address of logs is the IP address of the interface sending logs.

Writing Logs into Log Files

By default, logs are not written into log files. After the function of writing logs into log files is enabled, the level of logs written into log files is informational (Level 6) by default.

Run the **logging file flash:***filename* [*max-file-size*] [level] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log level.

Configuring the Interval at Which Logs Are Written into Log Files

By default, logs are written into log files at the interval of 3600s (one hour).

Run the **logging flash interval** *seconds* command in global configuration mode to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

By default, the storage time is not configured.

Run the **logging life-time level** *level days* command in global configuration mode to configure the storage time of logs. The administrator can specify different storage days for logs of different levels.

Immediately Writing Logs in the Buffer into Log Files

By default, syslogs are stored in the syslog buffer and then written into log files periodically or when the buffer is full.

Run the **logging flash flush** command in global configuration mode to immediately write logs in the buffer into log files so that you can collect logs conveniently.

7.3.4 Syslog Filtering

By default, logs generated by the system are sent in all directions.

Working Principle

Filtering Direction

Five log filtering directions are defined:

- **buffer**: Filters out logs sent to the log buffer, that is, logs displayed by the **show logging** command.
- **file**: Filters out logs written into log files.
- **server**: Filters out logs sent to the log server.

- **terminal**: Filters out logs sent to the Console and monitor terminal (including Telnet and SSH).

The four filtering directions can be used either in combinations to filter out logs sent in various directions, or separately to filter out logs sent in a single direction.

Filtering Mode

Two filtering modes are available:

- **contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are output. You may be interested in only a specified type of logs. In this case, you can apply the contains-only mode on the device to display only logs that match filtering rules on the terminal, helping you check whether any event occurs.
- **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be output. If a module generates too many logs, spamming may occur on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure related filtering rules to filter out logs that may cause spamming.

The two filtering modes are mutually exclusive, that is, you can configure only one filtering mode at a time.

Filter Rule

Two filtering rules are available:

- **exact-match**: If exact-match is selected, you must select all the three filtering options (module, level, and mnemonic). If you want to filter out a specified log, use the exact-match filtering rule.
- **single-match**: If exact-match is selected, you only need to select one of the three filtering options (module, level, and mnemonic). If you want to filter out a specified type of logs, use the single-match filtering rule.

If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Related Configuration

Configuring the Log Filtering Direction

By default, the log filtering direction is all, that is, logs sent in all directions are filtered.

Run the **logging filter direction** { **all** | **buffer | file** | **server | terminal** } command in global configuration mode to configure the log filtering direction to filter out logs in the specified directions.

Configuring the Log Filtering Mode

By default, the log filtering mode is filter-only.

Run the **logging filter type** { **contains-only** | **filter-only** } command in global configuration mode to configure the log filtering mode.

Configuring the Log Filtering Rule

By default, no log filtering rule is configured on a device, that is, logs are not filtered out.

Run the **logging filter rule exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* command in global configuration mode to configure the exact-match rule.

Run the **logging filter rule single-match** { **level** *level* **| mnemonic** *mnemonic-name* | **module** *module-name* } command in global configuration mode to configure the single-match rule.

7.3.5 Featured Logging

The featured logging functions include level-based logging, delayed logging, and periodical logging. If the RFC5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by default. If the RFC5424 log format is disabled, level-based logging, delayed logging, and periodical logging are disabled.

Working Principle

↘ Level-based Logging

You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure commands to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

↘ Delayed Logging

After generated, logs are not directly sent to the log server, and instead they are buffered in the log file. The device sends the log file to the syslog server through FTP at a certain interval. This function is called delayed logging.

If the device generates too many logs, sending all logs to the server in real time may deteriorate the performance of the device and the syslog server, and increase the burden of the network. In this case, the delayed logging function can be used to reduce the packet interaction.

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. By default, the file name prefix is syslog_ftp_server, the delayed logging interval is 3600s (one hour), and the log file size is 128 KB.

The maximum value of the delayed logging interval is 65535s, that is, 18 hours. If you set the delayed logging interval to the maximum value, the amount of logs generated in this period may exceed the file size (128 KB). To prevent loss of logs, logs will be written into a new log file, and the index increases by 1. When the timer expires, all log files buffered in this period will be sent to the FTP or TFTP server at a time.

The Flash on the device that is used to buffer the local log files is limited in size. A maximum of eight log files can be buffered on the device. If the number of local log files exceeds eight before the timer expires, all log files that are generated earlier will be sent to the FTP or TFTP server at a time.

↘ Periodical Logging

Logs about performance statistics are periodically sent. All periodical logging timers are managed by the syslog module. When the timer expires, the syslog module calls the log processing function registered with each module to output the

performance statistic logs and send logs in real time to the remote syslog server. The server analyzes these logs to evaluate the device performance.

By default, the periodical logging interval is 15 minutes. To enable the server to collect all performance statistic logs at a time, you need to set the log periodical logging intervals of different statistic objects to a common multiple of them. Currently, the interval can be set to 0, 15, 30, 60, or 120. 0 indicates that periodical logging is disabled.

Related Configuration

Configuring the Level-based Logging Policy

By default, device logs are sent in all directions.

Run the **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** } command in global configuration mode to configure the level-based logging policy.

Enabling Delayed Display of Logs on the Console and Remote Terminal

By default, delayed display of logs on the Console and remote terminal is disabled.

Run the **logging delay-send terminal** command in global configuration mode to enable delayed display of logs on the Console and remote terminal.

Configuring the Name of the File for Delayed Logging

By default, the log file sent to the remote server is named ***File size_Device IP address_Index*.txt**. If the prefix of the log file name is modified, the log file sent to the remote server is named ***Configured file name prefix_File size_Device IP address_Index*.txt**. The file stored on the local Flash of the device is named ***Configured file name prefix_Index*.txt**. The default file name prefix is syslog_ftp_server.

Run the **logging delay-send file flash:***filename* command in global configuration mode to configure the name of the log file that is buffered on the local device.

Configuring the Delayed Logging Interval

By default, the delayed logging interval is 3600s (one hour).

Run the **logging delay-send interval** *seconds* command in global configuration mode to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

By default, logs are not sent to any FTP or TFTP server.

Run the **logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** } command in global configuration mode to configure the server address and delayed logging mode.

Enabling Periodical Logging

By default, periodical logging is disabled.

Run the **logging statistic enable** command in global configuration mode to enable periodical uploading of logs. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

↘ Enabling Periodical Display of Logs on the Console and Remote Terminal

By default, periodical display of logs on the Console and remote terminal is disabled.

Run the **logging statistic terminal** command in global configuration mode to enable periodical display of logs on the Console and remote terminal.

↘ Configuring the Periodical Logging Interval

By default, the periodical logging interval is 15 minutes.

Run the **logging statistic mnemonic** *mnemonic* **interval** *minutes* command in global configuration mode to configure the periodical logging interval.

7.3.6 Syslog Monitoring

After syslog monitoring is enabled, the system monitors the access attempts of users and generates the related logs.

Working Principle

After logging of login/exit attempts is enabled, the system records the access attempts of users. The log contains user name and source address.

After logging of operations is enabled, the system records changes in device configurations, The log contains user name, source address, and operation.

Related Configuration

↘ Enabling Logging of Login or Exit Attempts

By default, a device does not generate logs when users access or exit the device.

Run the **logging userinfo** command in global configuration mode to enable logging of login/exit attempts. After this function is enabled, the device displays logs when users access the devices through Telnet, SSH, or HTTP so that the administrator can monitor the device connections.

↘ Enabling Logging of Operations

By default, a device does not generate logs when users modify device configurations.

Run the **logging userinfo command-log** command in global configuration mode to enable logging of operations. After this function is enabled, the system displays related logs to notify the administrator of configuration changes.

7.4 Configuration

Configuration	Description and Command

Configuration	Description and Command	
Configuring Syslog Format	(Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC5424 syslog format.
Sending Syslogs to the Console	(Optional) It is used to configure parameters for sending syslogs to the Console.	
	logging on	Enables logging.
	logging count	Enables log statistics.
	logging console [*level*]	Configures the level of logs displayed on the Console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the log rate limit.
Sending Syslogs to the Monitor Terminal	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the level of logs displayed on the monitor terminal.
Writing Syslogs into the Memory Buffer	(Optional) It is used to configure parameters for writing syslogs into the memory buffer.	
	logging buffered [*buffer-size*] [*level*]	Configures parameters for writing syslogs into the memory buffer, including the buffer size and log level.
Sending Syslogs to the Log Server	(Optional) It is used to configure parameters for sending syslogs to the log server.	
	logging server{ *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]	Sends logs to a specified log server.
	logging trap [*level*]	Configures the level of logs sent to the log server.
	logging facility *facility-type*	Configures the facility value of logs sent to the log server.
	logging source [**interface**] *interface-type interface-number*	Configures the source interface of logs sent to the log server.
	logging source { **ip** *ip-address* | **ipv6** *ipv6-address* }	Configures the source address of logs sent to the log server.

Configuration	Description and Command	
Writing Syslogs into Log Files	(Optional) It is used to configure parameters for writing syslogs into a file.	
	logging file flash:*filename* [*max-file-size*] [level]	Configures parameters for writing syslogs into a file, including the file storage type, file name, file size, and log level.
	logging flash interval *seconds*	Configures the interval at which logs are written into log files. The default value is 3600.
	logging life-time level *level days*	Configures the storage time of log files.
Configuring Syslog Filtering	(Optional) It is used to enable the syslog filtering function.	
	logging filter direction { **all** | **buffer | file | server | terminal** }	Configures the log filtering direction.
	logging filter type { **contains-only** | **filter-only** }	Configures the log filtering mode.
	logging filter rule exact-match module *module-name* **mnemonic** *mnemonic-name* **level** *level*	Configures the exact-match filtering rule.
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	Configures the single-match filtering rule.
Configuring Level-based Logging	(Optional) It is used to configure logging policies to send the syslogs based on module and severity level .	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	Sends logs to different destinations by module and severity level
Configuring Delayed Logging	(Optional) It is used to enable the delayed logging function.	
	logging delay-send terminal	Enables delayed display of logs on the Console and remote terminal.
	logging delay-send file flash:*filename*	Configures the name of the file on the local device where logs are buffered.
	logging delay-send interval *seconds*	Configures the interval at which logs are sent to the log server.
	logging delay-send server { *ip-address* | **ipv6** *ipv6-address* }**mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	Configures the server address and delayed logging mode.
Configuring Periodical Logging	(Optional) It is used to enable the periodical logging function.	
	logging statistic enable	Enables the periodical logging function .

Configuration	Description and Command	
	logging statistic terminal	Enables periodical display of logs on the Console and remote terminal.
	logging statistic mnemonic *mnemonic* **interval** *minutes*	Configures the interval at which logs of a performance statistic object are sent to the server .
Configuring Syslog Monitoring	(Optional) It is used to configure parameters of the syslog monitoring function .	
	logging userinfo	Enables logging of login/exit attempts.
	logging userinfo command-log	Enables logging of operations.

7.4.1 Configuring Syslog Format

Configuration Effect

- Configure the format of syslogs.

Notes

RFC3164 Log Format

- If the device does not have the real time clock (RTC), which is used to record the system absolute time, the device uses its startup time (uptime) as the syslog timestamp by default. If the device has the RTC, the device uses its absolute time (datetime) as the syslog timestamp by default.
- The log sequence number is a 6-digit integer. Each time a log is generated, the sequence number increases by one. Each time the sequence number increases from 000000 to 1,000,000, or reaches 2^32, the sequence number starts from 000000 again.

RFC5424 Log Format

- After the RFC5424 log format is enabled, the timestamp is uniform.
- In the RFC5424 log format, the timestamp may or may not contain the time zone. Currently, only the timestamp without the time zone is supported.

Configuration Steps

Configuring the Timestamp Format of Syslogs

- (Optional) By default, the datetime timestamp format is used.
- Unless otherwise specified, perform this configuration on the device to configure the timestamp format.

Adding the Sysname to the Syslog

- (Optional) By default, the syslog does not contain the sysname.
- Unless otherwise specified, perform this configuration on the device to add the sysname to the syslog.

Adding the Sequence Number to the Syslog

- (Optional) By default, the syslog does not contain the sequence number.
- Unless otherwise specified, perform this configuration on the device to add the sequence number to the syslog.

Enabling the Standard Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the standard log format.

Enabling the Private Log Format

- (Optional) By default, the default log format is used.
- Unless otherwise specified, perform this configuration on the device to enable the private log format.

Enabling the RFC5424 Log Format

- (Optional) By default, the RFC5424 log format is disabled.
- Unless otherwise specified, perform this configuration on the device to enable the RFC5424 log format.

Verification

- Generate a syslog, and check the log format.

Related Commands

Configuring the Timestamp Format of Syslogs

Command	**service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]
Parameter Description	*message-type*: Indicates the log type. There are two log types: log and debug. **uptime**: Indicates the device startup time in the format of dd:hh:mm:ss, for example, 07:00:10:41. **datetime**: Indicates the current device time in the format of MM DD hh:mm:ss, for example, Jul 27 16:53:07. **msec**: Indicates that the current device time contains millisecond. **year**: Indicates that the current device time contains year.
Command Mode	Global configuration mode
Configuration Usage	Two syslog timestamp formats are available, namely, uptime and datetime. You can select a timestamp format as required.

Adding the Sysname to the Syslog

Command	**service sysname**
Parameter Description	N/A
Command Mode	Global configuration mode

Configuration Usage	This command is used to add the sysname to the log to enable you to learn about the device that sends syslogs to the server.

Adding the Sequence Number to the Syslog

Command	**service sequence-numbers**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to add the sequence number to the log. The sequence number starts from 1. After the sequence number is added, you can learn clearly whether any log is lost and the generation sequence of logs.

Enabling the Standard Syslog Format

Command	**service standard-syslog**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logs are displayed in the following format (default format): `*timestamp: %module-level-mnemonic: content` If the standard syslog format is enabled, logs are displayed in the following format: `timestamp %module-level-mnemonic: content` Compared with the default format, an asterisk (*) is missing in front of the timestamp, and a colon (:) is missing at the end of the timestamp in the standard log format.

Enabling the Private Syslog Format

Command	**service private-syslog**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logs are displayed in the following format (default format): `*timestamp: %module-level-mnemonic: content` If the private syslog format is enabled, logs are displayed in the following format: `timestamp module-level-mnemonic: content` Compared with the default format, an asterisk (*) is missing in front of the timestamp, a colon (:) is missing at the end of the timestamp, and a percent sign (%) is missing in front of the module name in the private log

	format.

Enabling the RFC5424 Syslog Format

Command	**service log-format rfc5424**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After the new format (RFC5424 log format) is enabled, the **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** commands that are applicable only to the old format (RFC3164 log format) loss effect and are hidden. After the old format (RFC3164 log format) is enabled, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable only to the RFC5424 log format loss effect and are hidden. After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuration Example

Enabling the RFC3164 Log Format

Scenario	It is required to configure the timestamp format as follows: 1. Enable the RFC3164 format. 2. Change the timestamp format to datetime and add the millisecond and year to the timestamp. 3. Add the sysname to the log. 4. Add the sequence number to the log.
Configuration Steps	● Configure the syslog format.
	`Ruijie# configure terminal` `Ruijie(config)# no service log-format rfc5424` `Ruijie(config)# service timestamps log datetime year msec` `Ruijie(config)# service timestamps debug datetime year msec` `Ruijie(config)# service sysname` `Ruijie(config)# service sequence-numbers`
Verification	After the timestamp format is configured, verify that new syslogs are displayed in the RFC3164 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the timestamp in the new log.
	`Ruijie(config)#exit`

	001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console Ruijie#show logging config Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail

Enabling the RFC5424 Log Format

Scenario	It is required to enable the RFC5424 format.
Configuration Steps	● Configure the syslog format.
	Ruijie# configure terminal Ruijie(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in the RFC5424 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit global configuration mode to generate a new log, and check the format of the new log.
	Ruijie(config)#exit <133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console Ruijie#show logging config Syslog logging: enabled Console logging: level debugging, 4740 messages logged Monitor logging: level debugging, 0 messages logged

	Buffer logging: level debugging, 4745 messages logged Statistic log messages: disable Statistic log messages to terminal: disable Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds Count log messages: enable Trap logging: level informational, 2641 message lines logged,4155 fail logging to 192.168.23.89 logging to 2000::1 Delay-send logging: 2641 message lines logged logging to 192.168.23.89 by tftp

7.4.2 Sending Syslogs to the Console

Configuration Effect

- Send syslogs to the Console to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the Console.

Configuration Steps

Enabling Logging

- (Optional) By default, the logging function is enabled.

Enabling Log Statistics

- (Optional) By default, log statistics is disabled.
- Unless otherwise specified, perform this configuration on the device to enable log statistics.

Configuring the Level of Logs Displayed on the Console

- (Optional) By default, the level of logs displayed on the Console is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the Console.

Configuring the Log Rate Limit

- (Optional) By default, the no rate limit is configured.
- Unless otherwise specified, perform this configuration on the device to limit the log rate.

Verification

- Run the **show logging config** command to display the level of logs displayed on the Console.

Related Commands

Enabling Logging

Command	**logging on**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, logging is enabled. Do not disable logging in general cases. If too many syslogs are generated, you can configure log levels to reduce the number of logs.

Enabling Log Statistics

Command	**logging count**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, log statistics is disabled. If log statistics is enabled, syslogs will be classified and counted. The system records the number of times a log is generated and the last time when the log is generated.

Configuring the Level of Logs Displayed on the Console

Command	**logging console** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the Console is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs displayed on the Console.

Configuring the Log Rate Limit

Command	**logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]
Parameter Description	*number*: Indicates the maximum number of logs processed per second. The value ranges from 1 to 10,000. **all**: Indicates that rate limit is applied to all logs ranging from Level 0 to Level 7. **console**: Indicates the number of logs displayed on the Console per second. **except** *severity*: Rate limit is not applied to logs with a level equaling to or lower than the specified severity level. By default, the severity level is error (Level 3), that is, rate limit is not applied to logs of Level 3 or lower.

Command Mode	Global configuration mode
Configuration Usage	By default, no rate limit is configured.

Configuration Example

Sending Syslogs to the Console

Scenario	It is required to configure the function of displaying syslogs on the Console as follows: 1. Enable log statistics. 2. Set the level of logs that can be displayed on the Console to informational (Level 6). 3. Set the log rate limit to 50.
Configuration Steps	● Configure parameters for displaying syslogs on the Console.
	`Ruijie# configure terminal` `Ruijie(config)# logging count` `Ruijie(config)# logging console informational` `Ruijie(config)# logging rate-limit console 50`
Verification	● Run the **show logging config** command to display the configuration.
	`Ruijie(config)#show logging config` `Syslog logging: enabled` `  Console logging: level informational, 1303 messages logged` `  Monitor logging: level debugging, 0 messages logged` `  Buffer logging: level debugging, 1303 messages logged` `  File logging: level informational, 118 messages logged` `  File name:syslog_test.txt, size 128 Kbytes, have written 5 files` `  Standard format:false` `  Timestamp debug messages: datetime` `  Timestamp log messages: datetime` `  Sequence-number log messages: enable` `  Sysname log messages: enable` `  Count log messages: enable` `  Trap logging: level informational, 118 message lines logged,0 fail`

7.4.3 Sending Syslogs to the Monitor Terminal

Configuration Effect

- Send syslogs to a remote monitor terminal to facilitate the administrator to monitor the performance of the system.

Notes

- If too many syslogs are generated, you can limit the log rate to reduce the number of logs displayed on the monitor terminal.
- By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

Configuration Steps

↘ Allowing the Monitor Terminal to Display Logs

- (Mandatory) By default, the monitor terminal is not allowed to display logs.
- Unless otherwise specified, perform this operation on every monitor terminal connected to the device.

↘ Configuring the Level of Logs Displayed on the Monitor Terminal

- (Optional) By default, the level of logs displayed on the monitor terminal is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs displayed on the monitor terminal.

Verification

- Run the **show logging config** command to display the level of logs displayed on the monitor terminal.

Related Commands

↘ Allowing the Monitor Terminal to Display Logs

Command	**terminal monitor**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Configuration Usage	By default, the current monitor terminal is not allowed to display logs after you access the device remotely. You need to manually run the **terminal monitor** command to allow the current monitor terminal to display logs.

↘ Configuring the Level of Logs Displayed on the Monitor Terminal

Command	**logging monitor** [*level*]
Parameter Description	*level*: Indicates the log level.

Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs displayed on the monitor terminal is debugging (Level 7). You can run the **show logging config** command in privileged EXEC mode to display the level of logs displayed on the monitor terminal.

Configuration Example

↘ Sending Syslogs to the Monitor Terminal

Scenario	It is required to configure the function of displaying syslogs on the monitor terminal as follows: 1. Display logs on the monitor terminal. 2. Set the level of logs that can be displayed on the monitor terminal to informational (Level 6).
Configuration Steps	● Configure parameters for displaying syslogs on the monitor terminal.
	`Ruijie# configure terminal` `Ruijie(config)# logging monitor informational` `Ruijie(config)# line vty 0 4` `Ruijie(config-line)# monitor`
Verification	● Run the **show logging config** command to display the configuration.
	`Ruijie#show logging config` `Syslog logging: enabled` `  Console logging: level informational, 1304 messages logged` `  Monitor logging: level informational, 0 messages logged` `  Buffer logging: level debugging, 1304 messages logged` `  File logging: level informational, 119 messages logged` `  File name:syslog_test.txt, size 128 Kbytes, have written 5 files` `  Standard format:false` `  Timestamp debug messages: datetime` `  Timestamp log messages: datetime` `  Sequence-number log messages: enable` `  Sysname log messages: enable` `  Count log messages: enable` `  Trap logging: level informational, 119 message lines logged,0 fail`

Common Errors

- To disable this function, run the **terminal no monitor** command, instead of the **no terminal monitor** command.

7.4.4 Writing Syslogs into the Memory Buffer

Configuration Effect

- Write syslogs into the memory buffer so that the administrator can view recent syslogs by running the **show logging** command.

Notes

- If the buffer is full, old logs will be overwritten by new logs that are written into the memory buffer.

Configuration Steps

↘ Writing Logs into the Memory Buffer

- (Optional) By default, the system writes logs into the memory buffer, and the default level of logs is debugging (Level 7).
- Unless otherwise specified, perform this configuration on the device to write logs into the memory buffer.

Verification

- Run the **show logging config** command to display the level of logs written into the memory buffer.
- Run the **show logging** command to display the level of logs written into the memory buffer.

Related Commands

↘ Writing Logs into the Memory Buffer

Command	**logging buffered** [*buffer-size*] [*level*]
Parameter Description	*buffer-size*: Indicates the size of the memory buffer. *level*: Indicates the level of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs written into the memory buffer is debugging (Level 7). Run the **show logging** command in privileged EXEC mode to display the level of logs written into the memory buffer and the buffer size.

Configuration Example

↘ Writing Syslogs into the Memory Buffer

Scenario	It is required to configure the function of writing syslogs into the memory buffer as follows: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information level of logs that can be written into the memory buffer to informational (Level 6).
Configuration Steps	● Configure parameters for writing syslogs into the memory buffer.

	Ruijie# configure terminal Ruijie(config)# logging buffered 131072 informational
Verification	● Run the **show logging config** command to display the configuration and recent syslogs.
	Ruijie#show logging Syslog logging: enabled Console logging: level informational, 1306 messages logged Monitor logging: level informational, 0 messages logged Buffer logging: level informational, 1306 messages logged File logging: level informational, 121 messages logged File name:syslog_test.txt, size 128 Kbytes, have written 5 files Standard format:false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 121 message lines logged,0 fail Log Buffer (Total 131072 Bytes): have written 4200 001301: *Jun 14 2013 19:01:09.488: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console 001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console //Logs displayed are subject to the actual output of the **show logging** command.

7.4.5 Sending Syslogs to the Log Server

Configuration Effect

- Send syslogs to the log server to facilitate the administrator to monitor logs on the server.

Notes

- To send logs to the log server, you must add the timestamp and sequence number to logs. Otherwise, the logs are not sent to the log server.

Configuration Steps

Sending Logs to a Specified Log Server

- (Mandatory) By default, syslogs are not sent to any log server.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Level of Logs Sent to the Log Server

- (Optional) By default, the level of logs sent to the log server is informational (Level 6).
- Unless otherwise specified, perform this configuration on the device to configure the level of logs sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

- (Optional) If the RFC5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the log server is local0 (16) by default.
- Unless otherwise specified, perform this configuration on the device to configure the facility value of logs sent to the log server.

Configuring the Source Interface of Logs Sent to the Log Server

- (Optional) By default, the source interface of logs sent to the log server is the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source interface of logs sent to the log server.

Configuring the Source Address of Logs Sent to the Log Server

- (Optional) By default, the source address of logs sent to the log server is the IP address of the interface sending the logs.
- Unless otherwise specified, perform this configuration on the device to configure the source address of logs sent to the log server.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

Sending Logs to a Specified Log Server

Command	**logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*] Or **logging** { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*]
Parameter Description	*ip-address*: Specifies the IP address of the host that receives logs. **ipv6** *ipv6-address*: Specifies the IPv6 address of the host that receives logs. **udp-port** *port*: Specifies the port ID of the log server. The default port ID is 514.
Command Mode	Global configuration mode
Configuration	This command is used to specify the address of the log server that receives logs. You can specify multiple

Usage	log servers, and logs will be sent simultaneously to all these log servers. You can configure up to five log servers on a Ruijie product.

Configuring the Level of Logs Sent to the Log Server

Command	**logging trap** [*level*]
Parameter Description	*level*: Indicates the log level.
Command Mode	Global configuration mode
Configuration Usage	By default, the level of logs sent to the log server is informational (Level 6). You can run the **show logging config** command in privileged EXEC mode to display the level of logs sent to the log server.

Configuring the Facility Value of Logs Sent to the Log Server

Command	**logging facility** *facility-type*
Parameter Description	*facility-type*: Indicates the facility value of logs.
Command Mode	Global configuration mode
Configuration Usage	If the RFC5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC5424 format is enabled, the facility value of logs sent to the server is local0 (16) by default.

Configuring the Source Interface of Logs Sent to the Log Server

Command	**logging source** [**interface**] *interface-type interface-number*
Parameter Description	*interface-type*: Indicates the interface type. *interface-number*: Indicates the interface number.
Command Mode	Global configuration mode
Configuration Usage	By default, the source interface of logs sent to the log server is the interface sending the logs. To facilitate management, you can use this command to set the source interface of all logs to an interface so that the administrator can identify the device that sends the logs based on the unique address.

Configuring the Source Address of Logs Sent to the Log Server

Command	**logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* }
Parameter Description	**ip** *ip-address*: Specifies the source IPv4 address of logs sent to the IPv4 log server. **ipv6** *ipv6-address*: Specifies the source IPv6 address of logs sent to the IPv6 log server.
Command Mode	Global configuration mode
Configuration Usage	By default, the source IP address of logs sent to the log server is the IP address of the interface sending the logs.

	To facilitate management, you can use this command to set the source IP address of all logs to the IP address of an interface so that the administrator can identify the device that sends the logs based on the unique address..

Configuration Example

↘ Sending Syslogs to the Log Server

Scenario	It is required to configure the function of sending syslogs to the log server as follows: 1. Set the IPv4 address of the log server to 10.1.1.100. 2. Set the level of logs that can be sent to the log server to debugging (Level 7). 3. Set the source interface to Loopback 0.
Configuration Steps	● Configure parameters for sending syslogs to the log server.
	`Ruijie# configure terminal` `Ruijie(config)# logging server 10.1.1.100` `Ruijie(config)# logging trap debugging` `Ruijie(config)# logging source interface Loopback 0`
Verification	● Run the **show logging config** command to display the configuration.
	`Ruijie#show logging config` `Syslog logging: enabled` `  Console logging: level informational, 1307 messages logged` `  Monitor logging: level informational, 0 messages logged` `  Buffer logging: level informational, 1307 messages logged` `  File logging: level informational, 122 messages logged` `  File name:syslog_test.txt, size 128 Kbytes, have written 5 files` `  Standard format:false` `  Timestamp debug messages: datetime` `  Timestamp log messages: datetime` `  Sequence-number log messages: enable` `  Sysname log messages: enable` `  Count log messages: enable` `  Trap logging: level debugging, 122 message lines logged,0 fail` `    logging to  10.1.1.100`

7.4.6 Writing Syslogs into Log Files

Configuration Effect

- Write syslogs into log files at the specified interval so that the administrator can view history logs anytime on the local device.

Notes

- Sylsogs are not immediately written into log files. They are first buffered in the memory buffer, and then written into log files either periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Steps

Writing Logs into Log Files

- (Mandatory) By default, syslogs are not written to any log file.
- Unless otherwise specified, perform this configuration on every device.

Configuring the Number of Log Files

- (Optional) By default, syslogs are written to 16 log files.
- Unless otherwise specified, perform this configuration on the device to configure the number of files which logs are written into.

Configuring the Interval at Which Logs Are Written into Log Files

- (Optional) By default, syslogs are written to log files every hour.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs are written into log files.

Configuring the Storage Time of Log Files

- (Optional) By default, no storage time is configured.
- Unless otherwise specified, perform this configuration on the device to configure the storage time of log files.

Immediately Writing Logs in the Buffer into Log Files

- (Optional) By default, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full.
- Unless otherwise specified, perform this configuration to write logs in the buffer into log files immediately. This command takes effect only once after it is configured.

Verification

- Run the **show logging config** command to display the configurations related to the log server.

Related Commands

Writing Logs into Log Files

Command	**logging file** { **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } [*max-file-size*] [*level*]
Parameter Description	**flash**: Indicates that log files will be stored on the extended Flash. **usb0**: Indicates that log files will be stored on USB 0. This option is supported only when the device has one USB port and a USB flash drive is inserted into the USB port. **usb1**: Indicates that log files will be stored on USB 1. This option is supported only when the device has two USB ports and USB flash drives are inserted into the USB ports. **sd0**: Indicates that log files will be stored on the SD card. This option is supported only when the device has an SD port and an SD card is inserted into the SD port. *filename*: Indicates the log file name, which does not contain a file name extension. The file name extension is always txt. *max-file-size*: Indicates the maximum size of a log file. The value ranges from 128 KB to 6 MB. The default value is 128 KB. *level*: Indicates the level of logs that can be written into a log file.
Command Mode	Global configuration mode
Configuration Usage	This command is used to create a log file with the specified file name on the specified file storage device. The file size increases with the amount of logs, but cannot exceed the configured maximum size. If not specified, the maximum size of a log file is 128 KB by default. After this command is configured, the system saves logs to log files. A log file name does not contain any file name extension. The file name extension is always txt, which cannot be changed. After this command is configured, logs will be written into log files every hour. If you run the **logging flie flash:syslog** command, a total of 16 log files will be created, namely, **syslog.txt**, **syslog_1.txt**, **syslog_2.txt**, …, **syslog_14.txt**, and **syslog_15.txt**. Logs are written into the 16 log files in sequence. For example, the system writes logs into **syslog_1.txt** after **syslog.txt** is full. When **syslog_15.txt** is full, logs are written into **syslog.txt** again,

Configuring the Interval at Which Logs Are Written into Log Files

Command	**logging flash interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which logs are written into log files. The value ranges from 1s to 51,840s.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the interval at which logs are written into log files. The countdown starts after the command is configured.

Configuring the Storage Time of Log Files

Command	**logging life-time level** *level days*
Parameter Description	*level*: Indicates the log level. *days*: Indicates the storage time of log files. The unit is day. The storage time is not less than seven days.
Command Mode	Global configuration mode

Configuration Usage	After the log storage time is configured, the system writes logs of the same level that are generated in the same day into the same log file. The log file is named **yyyy-mm-dd_filename_level.txt**, where **yyyy-mm-dd** is the absolute time of the day when the logs are generated, **filename** is the log file named configured by the **logging file flash** command, and **level** is the log level. After you specify the storage time for logs of a certain level, the system deletes the logs after the storage time expires. Currently, the storage time ranges from 7days to 365 days. If the log storage time is not configured, logs are stored based on the file size to ensure compatibility with old configuration commands.

Immediately Writing Logs in the Buffer into Log Files

Command	**logging flash flush**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	After this command is configured, syslogs are stored in the buffer and then written into log files periodically or when the buffer is full. You can run this command to immediately write logs into log files. ⚠ The **logging flash flush** command takes effect once after it is configured. That is, after this command is configured, logs in the buffer are immediately written to log files.

Configuration Example

Writing Syslogs into Log Files

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	`Ruijie# configure terminal` `Ruijie(config)# logging file flash:syslog debugging` `Ruijie(config)# logging flash interval 600`
Verification	● Run the **show logging config** command to display the configuration.
	`Ruijie(config)#show logging config` `Syslog logging: enabled` `  Console logging: level informational, 1307 messages logged` `  Monitor logging: level informational, 0 messages logged`

Scenario	It is required to configure the function of writing syslogs into log files as follows: 1. Set the log file name to syslog. 2. Set the level of logs sent to the Console to debugging (Level 7). 3. Set the interval at which device logs are written into files to 10 minutes (600s).
Configuration Steps	● Configure parameters for writing syslogs into log files.
	`Ruijie# configure terminal` `Ruijie(config)# logging file flash:syslog debugging` `Ruijie(config)# logging flash interval 600`
Verification	● Run the **show logging config** command to display the configuration.
	`Buffer logging: level informational, 1307 messages logged` `File logging: level debugging, 122 messages logged` `File name:syslog.txt, size 128 Kbytes, have written 1 files` `Standard format:false` `Timestamp debug messages: datetime` `Timestamp log messages: datetime` `Sequence-number log messages: enable` `Sysname log messages: enable` `Count log messages: enable` `Trap logging: level debugging, 122 message lines logged,0 fail` `  logging to  10.1.1.100`

7.4.7 Configuring Syslog Filtering

Configuration Effect

- Filter out a specified type of syslogs if the administrator does not want to display these syslogs.
- By default, logs generated by all modules are displayed on the Console or other terminals. You can configure log filtering rules to display only desired logs.

Notes

- Two filtering modes are available: contains-only and filter-only. You can configure only one filtering mode at a time.
- If the same module, level, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule prevails over the exact-match rule.

Configuration Steps

↘ **Configuring the Log Filtering Direction**

- (Optional) By default, the filtering direction is all, that is, all logs are filtered out.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering direction.

Configuring the Log Filtering Mode

- (Optional) By default, the log filtering mode is filter-only.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering mode.

Configuring the Log Filtering Rule

- (Mandatory) By default, no filtering rule is configured.
- Unless otherwise specified, perform this configuration on the device to configure the log filtering rule.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Configuring the Log Filtering Direction

Command	**logging filter direction** { **all** | **buffer | file** | **server | terminal** }
Parameter Description	**all**: Filters out all logs. **buffer**: Filters out logs sent to the log buffer, that is, the logs displayed by the **show logging** command. **file**: Filters out logs written into log files. **server**: Filters out logs sent to the log server. **terminal**: Filters out logs sent to the Console and VTY terminal (including Telnet and SSH).
Command Mode	Global configuration mode
Configuration Usage	The default filtering direction is **all**, that is, all logs are filtered out. Run the **default logging filter direction** command to restore the default filtering direction.

Configuring the Log Filtering Mode

Command	**logging filter type** { **contains-only** | **filter-only** }
Parameter Description	**contains-only**: Indicates that only logs that contain keywords specified in the filtering rules are displayed. **filter-only**: Indicates that logs that contain keywords specified in the filtering rules are filtered out and will not be displayed.
Command Mode	Global configuration mode
Configuration Usage	Log filtering modes include contains-only and filter-only. The default filtering mode is filter-only.

Configuring the Log Filtering Rule

Command	**logging filter rule** { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* |

	single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }
Parameter Description	**exact-match**: If exact-match is selected, you must specify all three filtering options. **single-match**: If single-match is selected, you may specify only one of the three filtering options. **module** *module-name*: Indicates the module name. Logs of this module will be filtered out. **mnemonic** *mnemonic-name*: Indicates the mnemonic. Logs with this mnemonic will be filtered out. **level** *level*: Indicates the log level. Logs of this level will be filtered out.
Command Mode	Global configuration mode
Configuration Usage	Log filtering rules include exact-match and single-match. The **no logging filter rule exact-match** [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*] command is used to delete the exact-match filtering rules. You can delete all exact-match filtering rules at a time or one by one. The **no logging filter rule single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] command is used to delete the single-match filtering rules. You can delete all single-match filtering rules at a time or one by one.

Configuration Example

↘ Configuring Syslog Filtering

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.
	`Ruijie# configure terminal` `Ruijie(config)# logging filter direction server` `Ruijie(config)# logging filter direction terminal` `Ruijie(config)# logging filter type filter-only` `Ruijie(config)# logging filter rule single-match module SYS`
Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	`Ruijie#configure` `Enter configuration commands, one per line.  End with CNTL/Z.` `Ruijie(config)#exit` `Ruijie#` `Ruijie#show running-config | include logging`

Scenario	It is required to configure the syslog filtering function as follows: 1. Set the filtering directions of logs to **terminal** and **server.** 2. Set the log filtering mode to filter-only. 3. Set the log filtering rule to single-match to filter out logs that contain the module name "SYS".
Configuration Steps	● Configure the syslog filtering function.
	`Ruijie# configure terminal` `Ruijie(config)# logging filter direction server` `Ruijie(config)# logging filter direction terminal` `Ruijie(config)# logging filter type filter-only` `Ruijie(config)# logging filter rule single-match module SYS`
Verification	● Run the **show running-config | include loggging** command to display the configuration. ● Enter and exit global configuration mode, and verify that the system displays logs accordingly.
	`logging filter direction server` `logging filter direction terminal` `logging filter rule single-match module SYS`

7.4.8 Configuring Level-based Logging

Configuration Effect

- You can use the level-based logging function to send syslogs to different destinations based on different module and severity level. For example, you can configure a command to send WLAN module logs of Level 4 or lower to the log server, and WLAN module logs of Level 5 or higher to local log files.

Notes

- Level-based logging takes effect only when the RFC5424 format is enabled.

Configuration Steps

↘ Configuring Level-based Logging

- (Optional) By default, logs are sent in all directions.
- Unless otherwise specified, perform this configuration on the device to configure logging polices to send syslogs to different destinations based on module and severity level.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Configuring Level-based Logging

Command	**logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }
Parameter Description	*module-name*: Indicates the name of the module to which the logging policy is applied. **not-lesser-than**: If this option is specified, logs of the specified level or higher will be sent to the specified destination, and other logs will be filtered out. If this option is not specified, logs of the specified level or lower will be sent to the specified destination, and other logs will be filtered out. *level*: Indicates the level of logs for which the logging policy is configured. **all**: Indicates that the logging policy is applied to all logs. **server**: Indicates that the logging policy is applied only to logs sent to the log server. **file**: Indicates that the logging policy is applied only to logs written into log files. **console**: Indicates that the logging policy is applied only to logs sent to the Console. **monitor**: Indicates that the logging policy is applied only to logs sent to a remote terminal. **buffer**: Indicates that the logging policy is applied only to logs stored in the buffer.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure logging polices to send syslogs to different destinations based on module and severity level.

Configuration Example

Configuring Level-based Logging

Scenario	It is required to configure the logging policies as follows: 1. Send logs of Level 5 or higher that are generated by the system to the Console. 2. Send logs of Level 3 or lower that are generated by the system to the buffer.
Configuration Steps	● Configure the logging policies.
	`Ruijie# configure terminal` `Ruijie(config)# logging policy module SYS not-lesser-than 5 direction console` `Ruijie(config)# logging policy module SYS 3 direction buffer`
Verification	● Run the **show running-config | include logging policy** command to display the configuration. ● Exit and enter global configuration mode to generate a log containing module name “SYS”. Verify that the log is sent to the destination as configured.
	`Ruijie#show running-config | include logging policy` `logging policy module SYS not-lesser-than 5 direction console`

Scenario	It is required to configure the logging policies as follows: 1. Send logs of Level 5 or higher that are generated by the system to the Console. 2. Send logs of Level 3 or lower that are generated by the system to the buffer.
Configuration Steps	● Configure the logging policies.
	`Ruijie# configure terminal` `Ruijie(config)# logging policy module SYS not-lesser-than 5 direction console` `Ruijie(config)# logging policy module SYS 3 direction buffer`
Verification	● Run the **show running-config | include logging policy** command to display the configuration. ● Exit and enter global configuration mode to generate a log containing module name “SYS”. Verify that the log is sent to the destination as configured.
	`logging policy module SYS 3 direction buffer`

7.4.9 Configuring Delayed Logging

Configuration Effect

- By default, delayed logging is enabled by default at the interval of 3600s (one hour). The name of the log file sent to the remote server is ***File size_Device IP address_Index*.txt**. Logs are not sent to the Console or remote terminal.
- You can configure the interval based on the frequency that the device generates logs for delayed uploading. This can reduce the burden on the device, syslog server, and network. In addition, you can configure the name of the log file as required.

Notes

- This function takes effect only when the RFC5424 format is enabled.
- It is recommended to disable the delayed display of logs on the Console and remote terminal. Otherwise, a large amount of logs will be displayed, increasing the burden on the device.
- The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.
- If few logs are generated, you can set the interval to a large value so that many logs can be sent to the remote server at a time.

Configuration Steps

Enabling Delayed Display of Logs on Console and Remote Terminal

- (Optional) By default, delayed display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable delayed display of logs on the Console and remote terminal.

Configuring the Name of the File for Delayed Logging

- (Optional) By default, the name of the file for delayed logging is ***File size_Device IP address_Index*.txt**.
- Unless otherwise specified, perform this configuration on the device to configure the name of the file for delayed logging.

Configuring the Delayed Logging Interval

- (Optional) By default, the delayed logging interval is 3600s (one hour).
- Unless otherwise specified, perform this configuration on the device to configure the delayed logging interval.

Configuring the Server Address and Delayed Logging Mode

- (Optional) By default, log files are not sent to any remote server.
- Unless otherwise specified, perform this configuration on the device to configure the server address and delayed logging mode

Verification

- Run the **show running** command to display the configuration.

Related Commands

Enabling Delayed Display of Logs on Console and Remote Terminal

Command	**logging delay-send terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	N/A.

Configuring the Name of the File for Delayed Logging

Command	**logging delay-send file flash:***filename*
Parameter Description	**flash:***filename*: Indicates the name of the file on the local device where logs are buffered.
Command	Global configuration mode

Mode	
Configuration Usage	This command is used to configure the name of the file on the local device where logs are buffered. The file name cannot contain any dot (.) because the system automatically adds the index and the file name extension (.txt) to the file name when generating a locally buffered file. The index increases each time a new file is generated. In addition, the file name cannot contain characters prohibited by your file system, such as \, /, :, *, ", <, >, and |. For example, the configured file name is log_server, the current file index is 5, the file size is 1000 bytes, and the source IP address is 10.2.3.5. The name of the log file sent to the remote server is **log_server_1000_10.2.3.5_5.txt** while the name of the log file stored on the device is **log_server_5.txt**. If the source IP address is an IPv6 address, the colon (:) in the IPv6 address must be replaced by the hyphen (-) because the colon (:) is prohibited by the file system. For example, the file name is log_server, the current file index is 6, the file size is 1000 bytes, and the source IPv6 address is 2001::1. The name of the log file sent to the remote server is **log_server_1000_2001-1_6.txt** while the name of the log file stored on the device is **log_server_6.txt**.

Configuring the Delayed Logging Interval

Command	**logging delay-send interval** *seconds*
Parameter Description	*seconds*: Indicates the delayed logging interval. The unit is second.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the delayed logging interval. The value ranges from 600s to 65,535s.

Configuring the Server Address and Delayed Logging Mode

Command	**logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* }**mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }
Parameter Description	*ip-address*: Indicates the IP address of the server that receives logs. **ipv6** *ipv6-address*: Indicates the IPv6 address of the server that receives logs. *username*: Specifies the user name of the FTP server. *password*: Specifies the password of the FTP server. **0**: (Optional) Indicates that the following password is in plain text. **7**: Indicates that the following password is encrypted.
Command Mode	Global configuration mode
Configuration Usage	This command is used to specify an FTP or a TFTP server for receiving the device logs. You can configure a total of five FTP or TFTP servers, but a server cannot be both an FTP and TFTP server.. Logs will be simultaneously sent to all FTP or TFTP servers.

Configuration Example

Configuring Delayed Logging

Scenario	It is required to configure the delayed logging function as follows: 1. Enable the delayed display of logs on the Console and remote terminal. 2. Set the delayed logging interval to 7200s (two hours). 3. Set the name of the file for delayed logging to syslog_ruijie. 4. Set the IP address of the server to 192.168.23.12, user name to admin, password to admin, and logging mode to FTP.
Configuration Steps	● Configure the delayed logging function.
	`Ruijie# configure terminal` `Ruijie(config)# logging delay-send terminal` `Ruijie(config)# logging delay-send interval 7200` `Ruijie(config)# logging delay-send file flash:syslog_ruijie` `Ruijie(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin`
Verification	● Run the **show running-config | include logging delay-send** command to display the configuration. ● Verify that logs are sent to the remote FTP server after the timer expires.
	`Ruijie#show running-config | include logging delay-send` `logging delay-send terminal` `logging delay-send interval 7200` `logging delay-send file flash:syslog_ruijie` `logging delay-send server 192.168.23.12 mode ftp user admin password admin`

7.4.10 Configuring Periodical Logging

Configuration Effect

- By default, periodical logging is disabled. Periodical logging interval is 15 minutes. Periodical display of logs on the Console and remote terminal are disabled.
- You can modify the periodical logging interval. The server will collect all performance statistic logs at the time point that is the least common multiple of the intervals of all statistic objects.

Notes

- Periodical logging takes effect only when the RFC5424 format is enabled.
- The settings of the periodical logging interval and the function of displaying logs on the Console and remote terminal take effect only when the periodical logging function is enabled.
- It is recommended to disable periodical display of logs on the Console and remote terminal. Otherwise, a large amount of performance statistic logs will be displayed, increasing the burden on the device.

- To ensure the server can collect all performance statistic logs at the same time point, the timer will be restarted when you modify the periodical logging interval of a statistic object.

Configuration Steps

Enabling Periodical Logging

- (Optional) By default, periodical logging is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical logging.

Enabling Periodical Display of Logs on Console and Remote Terminal

- (Optional) By default, periodical display of logs on the Console and remote terminal is disabled.
- Unless otherwise specified, perform this configuration on the device to enable periodical display of logs on the Console and remote terminal.

Configuring the Periodical Logging Interval

- (Optional) By default, the periodical logging interval is 15 minutes.
- Unless otherwise specified, perform this configuration on the device to configure the interval at which logs of statistic objects are sent to the server.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Enabling Periodical Logging

Command	**logging statistic enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	This command is used to enable periodical logging. After this function is enabled, the system outputs a series of performance statistics at a certain interval so that the log server can monitor the system performance.

Enabling Periodical Display of Logs on Console and Remote Terminal

Command	**logging statistic terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration	N/A

Usage	

Configuring the Periodical Logging Interval

Command	**logging statistic mnemonic** *mnemonic* **interval** *minutes*
Parameter Description	*mnemonic*: Identifies a performance statistic object. *minutes*: Indicates the periodical logging interval. The unit is minute.
Command Mode	Global configuration mode
Configuration Usage	This command is used to configure the periodical logging interval for a specified performance statistic object. The interval can be set to 0, 15, 30, 60, or 120 minutes. 0 indicates that periodical logging is disabled.

Configuration Example

Configuring Periodical Logging

Scenario	It is required to configure the l periodical logging function as follows: 1. Enable the periodical logging function. 2. Enable periodical display of logs on the Console and remote terminal. 3. Set the periodical logging interval of the statistic object TUNNEL_STAT to 30 minutes.
Configuration Steps	● Configure the periodical logging function.
	`Ruijie# configure terminal` `Ruijie(config)# logging statistic enable` `Ruijie(config)# logging statistic terminal` `Ruijie(config)# logging statistic mnemonic TUNNEL_STAT interval 30`
Verification	● Run the **show running-config	include logging statistic** command to display the configuration. ● After the periodical logging timer expires, verify that logs of all performance statistic objects are generated at the time point that is the least common multiple of the intervals of all statistic objects.
	`Ruijie#show running-config	include logging statistic` `logging statistic enable` `logging statistic terminal` `logging statistic mnemonic TUNNEL_STAT interval 30`

7.4.11 Configuring Syslog Monitoring

Configuration Effect

- Record login/exit attempts. After logging of login/exit attempts is enabled, the related logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator monitor the device connections.

- Record modification of device configurations. After logging of operations is enabled, the related logs are displayed on the device when users modify the device configurations. This helps the administrator monitor the changes in device configurations.

Notes

- If both the **logging userinfo** command and the **logging userinfo command-log** command are configured on the device, only the configuration result of the **logging userinfo command-log** command is displayed when you run the **show running-config** command.

Configuration Steps

Enabling Logging of Login/Exit Attempts

- (Optional) By default, logging of login/exit attempts is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of login/exit attempts.

Enabling logging of Operations

- (Optional) By default, logging of operations is disabled.
- Unless otherwise specified, perform this configuration on every line of the device to enable logging of operations.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Enabling Logging of Login/Exit Attempts

Command	**logging userinfo**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration Usage	By default, a device does not generate related logs when users log into or exit the device.

Enabling Logging of Operations

Command	**logging userinfo command-log**
Parameter Description	N/A
Command Mode	Global configuration mode
Configuration	The system generates related logs when users run configuration commands. By default, a device does not

Usage	generate logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

Scenario	It is required to configure the syslog monitoring function as follows: 1. Enable logging of login/exit attempts. 2. Enable logging of operations.
Configuration Steps	● Configure the syslog monitoring function.
	Ruijie# configure terminal Ruijie(config)# logging userinfo Ruijie(config)# logging userinfo command-log
Verification	● Run the **show running-config | include logging** command to display the configuration. ● Run a command in global configuration mode, and verify that the system generates a log.
	Ruijie#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#interface gigabitEthernet 0/0 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/0 Ruijie#show running-config | include logging logging userinfo command-log

7.4.12 Synchronizing User Input with Log Output

Configuration Effect

- By default, the user input is not synchronized with the log output. After this function is enabled, the content input during log output is displayed after log output is completed, ensuring integrity and continuity of the input.

Notes

- This command is executed in line configuration mode. You need to configure this command on every line as required.

Configuration Steps

Synchronizing User Input with Log Output

- (Optional) By default, the synchronization function is disabled.
- Unless otherwise specified, perform this configuration on every line to synchronize user input with log output.

Verification

- Run the **show running** command to display the configuration.

Related Commands

Synchronizing User Input with Log Output

Command	logging synchronous
Parameter Description	N/A
Command Mode	Line configuration mode
Configuration Usage	This command is used to synchronize the user input with log output to prevent interrupting the user input.

Configuration Example

Synchronizing User Input with Log Output

Scenario	It is required to synchronize the user input with log output as follows: 1. Enable the synchronization function.
Configuration Steps	● Configure the synchronization function.
	Ruijie# configure terminal Ruijie(config)# line console 0 Ruijie(config-line)# logging synchronous
Verification	● Run the **show running-config | begin line** command to display the configuration.
	Ruijie#show running-config | begin line line con 0 logging synchronous login local As shown in the following output, when a user types in "vlan", the state of interface 0/1 changes and the related log is output. After log output is completed, the log module automatically displays the user input "vlan" so that the user can continue typing. Ruijie(config)#vlan *Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up *Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up Ruijie(config)#vlan

7.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears logs in the memory buffer.	**clear logging**

Displaying

Description	Command
Displays log statistics and logs in the memory buffer based on the timestamp from oldest to latest.	**show logging**
Displays log statistics and logs in the memory buffer based on the timestamp from latest to oldest.	**show logging reverse**
Displays syslog configurations and statistics.	**show logging config**
Displays log statistics of each module in the system.	**show logging count**

8 Configuring CWMP

8.1 Overview

CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, related message specifications, management methods, and data models, so as to solve difficulties in unified management and maintenance of dispersed customer-premises equipment (CPEs), improve troubleshooting efficiency, and save O&M costs.

CWMP provides the following functions:

- **Auto configuration and dynamic service provisioning.** CWMP allows an Auto-Configuration Server (ACS) to automatically provision CPEs who initially access the network after start. The ACS can also dynamically re-configure running CPEs.
- **Firmware management.** CWMP manages and upgrades the firmware and its files of CPEs.
- **Software module management.** CWMP manages modular software according to data models implemented.
- **Status and performance monitoring.** CWMP enables CPEs to notify the ACE of its status and changes, achieving real-time status and performance monitoring.
- **Diagnostics.** The ACE diagnoses or resolves connectivity or service problems based on information from CPEs, and can also perform defined diagnosis tests.

Protocols and Standards

For details about TR069 protocol specifications, visit http://www.broadband-forum.org/technical/trlist.php.

Listed below are some major CWMP protocol specifications:

- TR-069_Amendment-4.pdf: CWMP standard
- TR-098_Amendment-2.pdf: Standard for Internet gateway device data model
- TR-106_Amendment-6.pdf: Standard for CPE data model
- TR-181_Issue-2_Amendment-5.pdf: Standard for CPE data model 2
- tr-098-1-4-full.xml: Definition of Internet gateway device data model
- tr-181-2-4-full.xml: Definition 2 of CPE data model 2

8.2 Applications

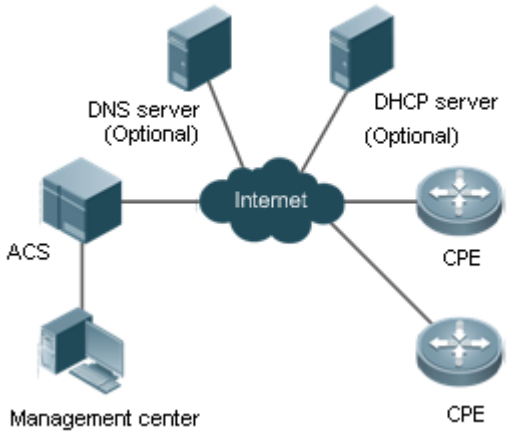
Typical Application	Scenario
CWMP Network Application Scenario	Initiate CPE-ACS connection, so as to upgrade the CPE firmware, upload the configuration files, restore the configuration, and realize other features.

8.2.1 CWMP Network Application Scenario

Application Scenario

The major components of a CWMP network architecture are CPEs, an ACS, a management center, a DHCP server, and a Domain Name System (DNS) server. The management center manages a population of CPEs by controlling the ACS on a Web browser.

Figure 8-1



Note	● If the Uniform Resource Locator (URL) of the ACS is configured on CPEs, the DHCP server is optional. If not, the DHCP is required to dynamically discover the ACS URL. ● If the URLs of the ACS and CPEs contain IP addresses only, the DNS server is optional. If their URLs contain domain names, the DNS server is required to resolves the names.

Functional Deployment

HTTP runs on both CPEs and the ACS.

8.3 Features

Basic Concept

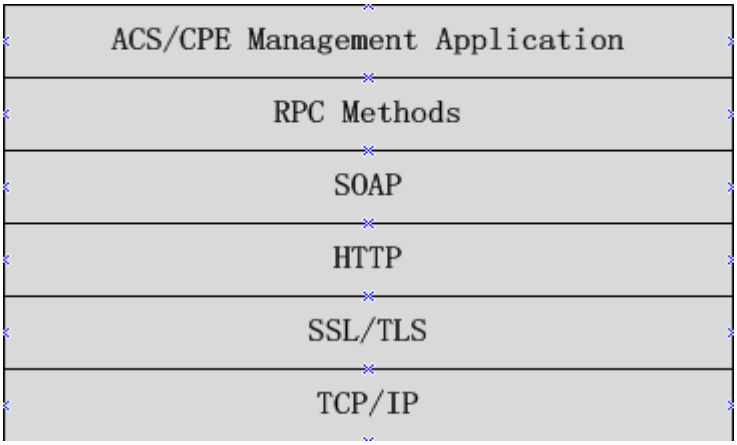
↘ Major Terminologies

- **CPE**: Customer Premises Equipment
- **ACS**: Auto-Configuration Server
- **RPC**: Remote Procedure Call
- **DM**: Data Model

Protocol Stack

Figure 8-2 shows the protocol stack of CWMP.

Figure 8-2 CWMP Protocol Stack



As shown in figure 8-2, CWMP defines six layers with respective functions as follows:

- ACS/CPE Application

The application layer is not a part of CWMP. It is the development performed by various modules of the CPEs/ACS to support CWMP, just like the Simple Network Management Protocol (SNMP), which does not cover the MIB management of functional modules.

- RPC Methods

This layer provides various RPC methods for interactions between the ACS and the CPEs.

- SOAP

The Simple Object Access Protocol (SOAP) layer uses a XML-based syntax to encode and decode CWMP messages.. Thus, CWMP messages must comply with the XML-based syntax.

- HTTP

All CWMP messages are transmitted over Hypertext Transfer Protocol (HTTP). Both the ACS and the CPEs can behave in the role of HTTP clients and servers. The server function is used to monitor reverse connections from the peer.

- SSL/TLS

The Secure Sockets Layer (SSL) or Transport Layer Security (TLS) layer guarantees CWMP security, including data integrity, confidentiality, and authentication.

- TCP/IP

This layer is the (Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack.

RPC Methods

The ACS manages and monitors CPEs by calling mostly the following RPC methods:

- Get RPC Methods

The Get methods enable the ACS to remotely obtain the set of RPC methods, as well as names, values and attributes of the DM parameters supported on CPEs.

- Set RPC Methods

The Set methods enable the ACS to remotely set the values and attributes of the DM parameters supported on CPEs.

- Inform RPC Methods

The Inform methods enable CPEs to inform the ACS of their device identifiers, parameter information, and events whenever sessions are established between them.

- Download RPC Methods

The Download method enables the ACS to remotely control the file download of CPEs, including firmware management, upgrade, and Web package upgrade.

- Upload RPC Methods

The Upload method enables the ACS to remotely control the file upload of CPEs, including upload of firmware and logs.

- Reboot RPC Methods

The Reboot method enables the ACS to remotely reboot the CPEs.

Session Management

CWMP sessions or interactions are the basis for CWMP. All CWMP interactions between the ACS and CPEs rely on their sessions. CWMP helps initiate and maintain ACS-CPE sessions to link them up for effective management and monitoring. An ACS-CPE session is a TCP connection, which starts from the Inform negotiation to TCP disconnection. The session is classified into CPE Initiated Session and ACS Initiated Session according to the session poster.

DM Management

CWMP operates based on CWMP Data Model (DM). CWMP manages all functional modules by a set of operations performed on DM. Each functional module registers and implements a respective data model, just like the MIBs implemented by various functional modules of SNMP.

A CWMP data model is represented in the form of a character string. For a clear hierarchy of the data model, a dot (.) is used as a delimiter to distinguish an upper-level data model node from a lower-level data model node. For instance, in the data model **InternetGatewayDevice.LANDevice**, **InternetGatewayDevice** is the parent data model node of **LANDevice**, and **LANDevice** is the child data model node of **InternetGatewayDevice**.

DM nodes are classified into two types: object nodes and parameter nodes. The parameter nodes are also known as leaf nodes. An object node is a node under which there are child nodes, and a parameter node is a leaf node under which there is no any child node. Object nodes are further classified into single-instance object nodes and multi-instance object nodes. A single-instance object node is an object node for which there is only one instance, whereas a multi-instance object node is an object node for which there are multiple instances.

DM nodes can also be classified into readable nodes and readable-and-writable nodes. A readable node is a node whose parameter values can be read but cannot be modified, and a readable-and-writable node is a node whose parameter values can be both read and modified.

A data model node has two attributes. One attribute relates to a notification function; that is, whether to inform the ACS of changes (other than changes caused by CWMP) to parameter values of the data model. The other attribute is an identifier indicating that the parameters of the data model node can be written using other management modes (than the ACS); that is, whether the values of the parameters can be modified using other management modes such as Telnet. The ACS can modify the attributes of the data models using RPC methods.

CWMP manages the data models using corresponding RPC methods.

↘ Event Management

When some events concerned by the ACS occur on the CPE, the CPE will inform the ACS of these events. The ACS monitors these events to monitor the working status of the CPE. The CWMP events are just like Trap messages of SNMP or product logs. Using RPC methods, to the ACS filters out the unconcerned types of events. CWMP events are classified into two types: single or (not cumulative) events and multiple (cumulative) events. A single event means that there is no quantitative change to the same event upon re-occurrence of the event, with the old discarded and the newest kept. A multiple event means that the old are not discarded and the newest event is kept as a complete event when an event re-occurs for multiple times later; that is, the number of this event is incremented by 1.

All events that occur on the CPE are notified to the ACS using the INFORM method.

Features

Feature	Description
Upgrading the Firmware	The ACS controls the upgrade of the firmware of a CPE using the Download method.
Upgrading the Configuration Files	The ACS controls the upgrade of the configuration files of a CPE using the Download method.
Uploading the Configuration Files	The ACS controls the upload of the configuration files of a CPE using the Upload method.
Backing up and Restoring a CPE	When a CPE breaks away from the management center, this feature can remotely restore the CPE to the previous status.

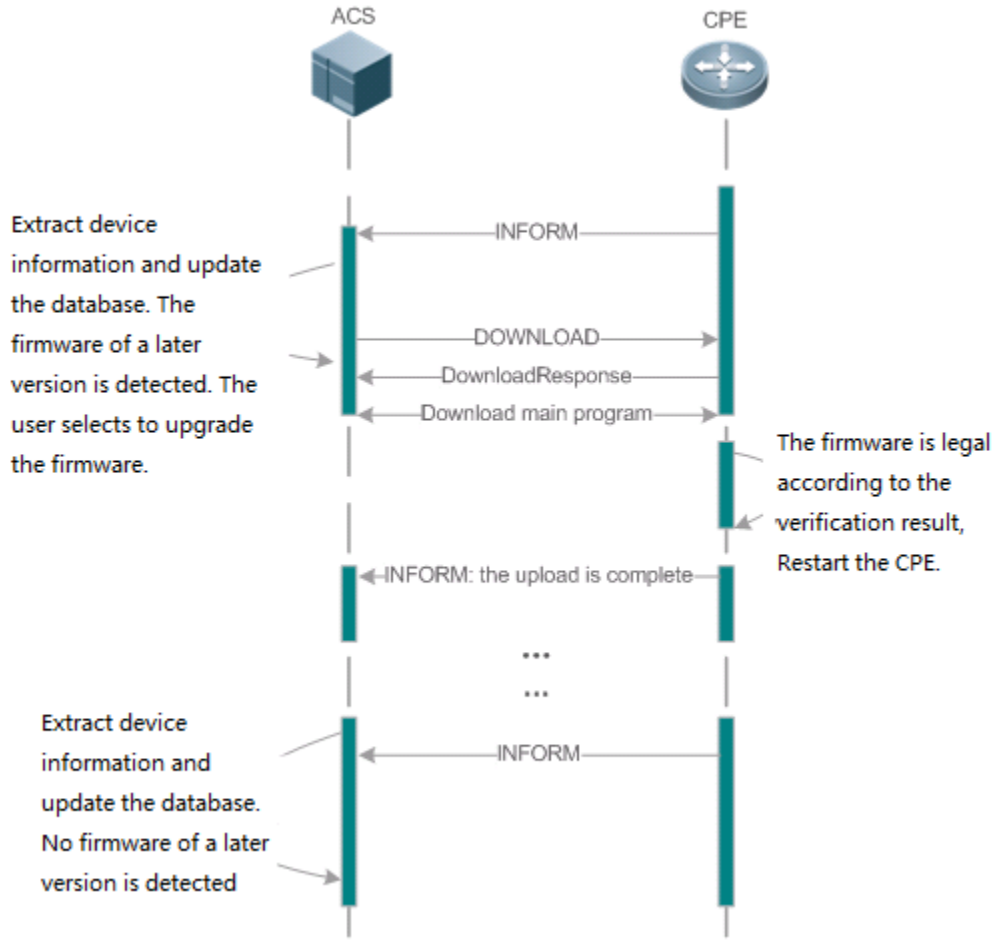
8.3.1 Upgrading the Firmware

Upgrading the Firmware means the firmware of a network element (NE) can be upgraded, so as to implement device version upgrade or replacement.

Working Principle

↘ Sequence Diagram of Upgrading the Firmware

Figure 8-3



Users specify a CPE for the ACS to deliver the Download method for upgrading the firmware. The CPE receives the request and starts to download the latest firmware from the destination file server, upgrade the firmware, and then reboot. After restart, the CPE will indicate the successful or unsuccessful completion of the method application.

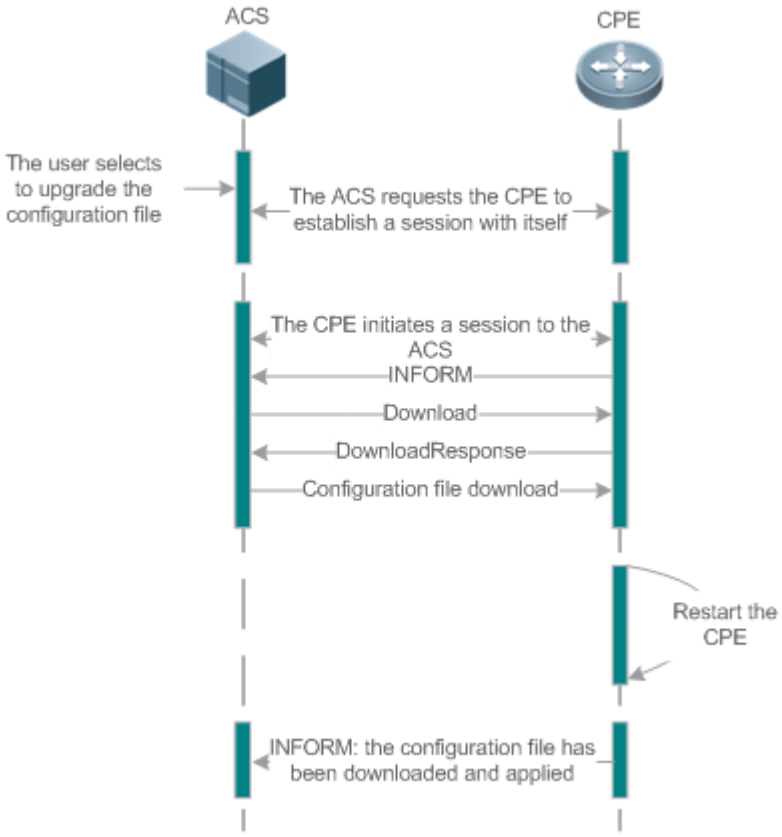
The file server can be ACS or separately deployed.

8.3.2 Upgrading the Configuration Files

Upgrading the Configuration Files means the current configuration files of a CPE can be replaced with specified configuration files, so that the new configuration files act on the CPE after reset.

Working Principle

Figure 8-4



Users specify a CPE for the ACS to deliver the Download methods for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. After that, the CPE will indicate successful or unsuccessful completion of the method application.

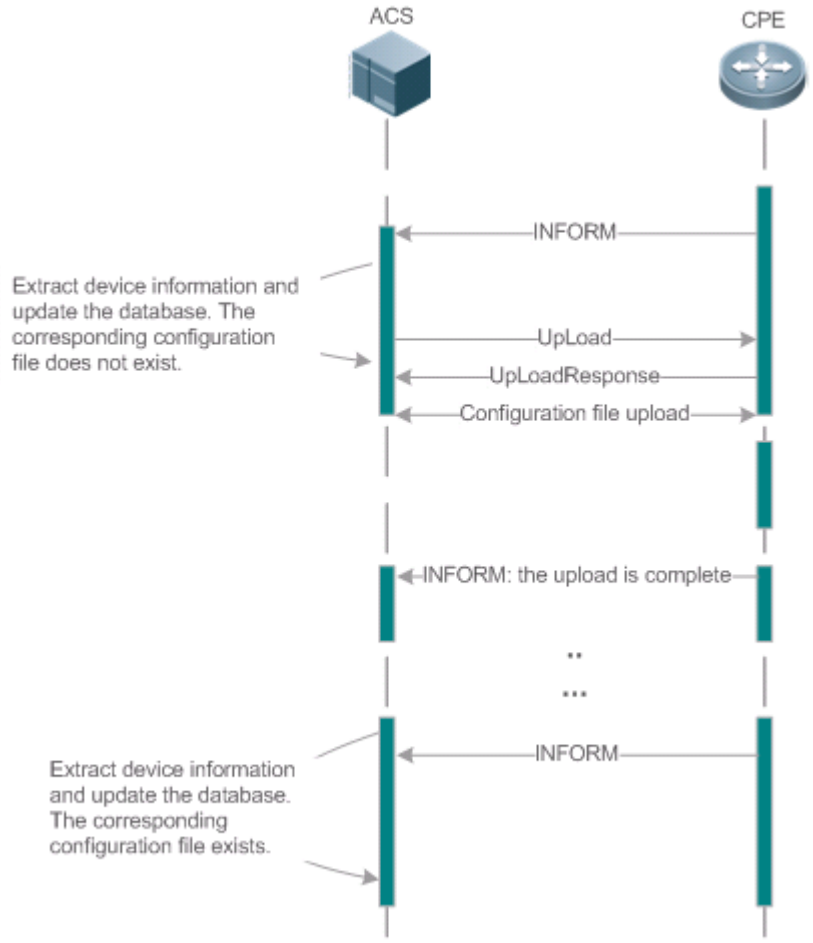
The file server can be ACS or separately deployed.

8.3.3 Uploading the Configuration Files

Uploading the Configuration Files means the ACS controls the configuration files of CPEs by using the Upload method.

Working Principle

Figure 8-5



When a CPE initially accesses the ACS, the ACS attempts to learn the configuration files of the CPE in the following sequence:

- When the ACS initially receives an Inform message from the CPE, it locates the corresponding database information according to device information carried in the message.
- If the database does not contain the configuration files of the CPE, the ACS delivers the Upload method to the CPE for uploading the configuration files.
- The CPE uploads its current configuration files to the ACS.
- The CPE returns a successful or unsuccessful response to the Upload request.

8.3.4 Backing Up and Restoring a CPE

When a remote CPE breaks away from the management center due to abnormal operations, the CPE backup and restoration feature helps restore the CPE to the previous status, so that the management center can resume the supervision of the CPE as necessary.

Working Principle

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its firmware or configuration files. Then when the CPE fails to connect to the ACS and breaks away from the management center after its firmware or configuration files are upgraded, the previous firmware or configuration files of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong version or configuration file.

Before the CPE receives a new firmware or configuration files to upgrade, the CPE will back up its current version and configuration files. In addition, there is a mechanism for determining whether the problem described in the preceding scenario has occurred. If the problem has occurred, the CPE is restored to the previous manageable status.

8.4 Configuration

Action	Suggestions and Related Commands	
Establishing a Basic CWMP Connection	⚠ (Mandatory) You can configure the ACS or CPE usernames and passwords to be authenticated for CWMP connection.	
	cwmp	Enables CWMP and enters CWMP configuration mode.
	acs username	Configures the ACS username for CWMP connection.
	acs password	Configures the ACS password for CWMP connection.
	cpe username	Configures the CPE username for CWMP connection.
	cpe password	Configures the CPE password for CWMP connection.
	⚠ (Optional) You can configure the URLs of the CPE and the ACS.	
	acs url	Configures the ACS URL.
	cpe url	Configures the CPE URL.
Configuring CWMP-Related Attributes	⚠ (Optional) You can configure the basic functions of the CPE, such as upload, backup and restoration of firmware, configuration files or logs.	
	cpe inform	Configures the periodic notification function of the CPE.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	disable download	Disables the function of downloading firmware and configuration files from the ACS.

Action	Suggestions and Related Commands	
	disable upload	Disables the function of uploading configuration and log files to the ACS.
	timer cpe- timeout	Configures the ACS response timeout on CPEs.

8.4.1 Establishing a Basic CWMP Connection

Configuration Effect

- A session connection is established between the ACS and the CPE.

Precautions

- N/A

Configuration Method

Enabling CWMP and Entering CWMP Configuration Mode

- (Mandatory) The CWMP function is enabled by default.

Command	**cwmp**
Parameter Description	N/A
Defaults	CWMP is enabled by default.
Command Mode	Global configuration guide
Usage Guide	N/A

Configuring the ACS Username for CWMP Connection

- This configuration is mandatory on the ACS.
- Only one username can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs username** *username*
Parameter Description	**username** *username*: The ACS username for CWMP connection
Defaults	The ACS username is not configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Password for CWMP Connection

- This configuration is mandatory on the ACS.

- The password of the ACS can be in plaintext or encrypted form. Only one password can be configured for the ACS. If multiple are configured, the latest configuration is applied.

Command	**acs password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password:* ACS password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Username for CWMP Connection

- This configuration is mandatory on the CPE.
- Only one username can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe username** *username*
Parameter Description	*username*: CPE username
Defaults	No CPE username is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Password for CWMP Connection

- This configuration is mandatory on the CPE.
- The password of the CPE can be in plaintext or encrypted form. Only one password can be configured for the CPE. If multiple are configured, the latest configuration is applied.

Command	**cpe password** {*password* **|** *encryption-type encrypted-password*}
Parameter Description	*password:* CPE password *encryption-type:* 0 (no encryption) or 7 (simple encryption) *encrypted-password:* Password text
Defaults	*encryption-type*: 0 *encrypted-password*: N/A
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

	● Contain 1 to 26 characters including letters and figures. ● The leading spaces will be ignored, while the trailing and middle are valid. ● If 7 (simple encryption) is specified, the valid characters only include 0 to 9 and a (A) to f (F).

Configuring the ACS URL for CMWP Connection

- This configuration is optional on the CPE.
- Only one ACS URL can be configured. If multiple are configured, the latest configuration is applied. The ACS URL must be in HTTP format.

Command	**acs url** *url*
Parameter Description	*url*: ACS URL
Defaults	No ACS URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If the ACS URL is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate connection to the ACS. The ACS URL must: ● Be in format of **http://host[:port]/path** or **https://host[:port]/path**. ● Contain 255 characters at most.

Configuring the CPE URL for CWMP Connection

- This configuration is optional on the CPE.
- Only one CPE URL can be configured. If multiple are configured, the latest configuration is applied. The CPE URL must be in HTTP format instead of domain name format.

Command	**cpe url** *url*
Parameter Description	*url:* CPE URL
Defaults	No CPE URL is configured by default.
Command Mode	CWMP configuration mode
Usage Guide	If CPE URL is not configured, it is obtained through DHCP. The CPE URL must: ● Be in format of **http://ip [: port]/**. ● Contain 255 characters at most.

Verification

- Run the **show cwmp configuration** command.

Command	**show cwmp configuration**
Parameter Description	N/A
Command	Privileged EXEC mode

Mode	
Usage Guide	N/A
Configuration Examples	The following example displays the CWMP configuration. `Ruijie(config-cwmp)#show cwmp configuration` `CWMP Status : enable` `ACS URL : http://www.ruijie.com.cn/acs` `ACS username : admin` `ACS password : ******` `CPE URL : http://10.10.10.2:7547/` `CPE username : ruijie` `CPE password : ******` `CPE inform status : disable` `CPE inform interval : 60s` `CPE inform start time : 0:0:0 0 0 0` `CPE wait timeout : 50s` `CPE download status : enable` `CPE upload status : enable` `CPE back up status : enable` `CPE back up delay time : 60s`

Configuration Examples

The following configuration examples describe CWMP-related configuration only.

Configuring Usernames and Passwords on the CPE

Network Environment Figure 8-6	
Configuration Method	● Enable CWMP. ● On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. ● On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to the CPE.
CPE	`Ruijie# configure terminal` `Enter configuration commands, one per line. End with CNTL/Z.` `Ruijie(config)# cwmp` `Ruijie(config-cwmp)# acs username USERB` `Ruijie(config-cwmp)# acs password PASSWORDB` `Ruijie(config-cwmp)# cpe username USERB` `Ruijie(config-cwmp)# cpe password PASSWORDB`
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been

	successfully applied.
CPE	Ruijie # show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : USERB CPE password : ******

↘ Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 8-6.
Configuration Method	● Configure the ACS URL. ● Configure the CPE URL.
CPE	Ruijie# configure terminal Ruijie(config)# cwmp Ruijie(config-cwmp)# acs url http://10.10.10.1:7547/acs Ruijie(config-cwmp)# cpe url http://10.10.10.1:7547/
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration CWMP Status : enable ACS URL : http://10.10.10.1:7547/acs ACS username : USERA ACS password : ****** CPE URL : http://10.10.10.1:7547/

Common Errors

- The user-input encrypted password is shorter than 2 characters or longer than 254 characters, or the length of the password is not an even number.
- The user-input plaintext password is longer than 126 characters.
- The user-input plaintext password contains illegal characters.
- The URL of the ACS is set to **NULL**.
- The URL of the CPE is set to **NULL**.

8.4.2 Configuring CWMP-Related Attributes

Configuration Effect

- You can configure common functions of the CPE, such as the backup and restoration of its firmware or configuration file, whether to enable the CPE to download firmware and configuration files from the ACS, and whether to enable the CPE to upload its configuration and log files to the ACS.

Configuration Method

Configuring the Periodic Notification Function of the CPE

- (Optional) The value range is from 30 to 3,600 in seconds. The default value is 600 seconds.
- Perform this configuration to reset the periodical notification interval of the CPE.

Command	**cpe inform** [**interval** *seconds*] [**starttime** *time*]
Parameter Description	*seconds*: Specifies the periodical notification interval of the CPE. The value range is from 30 to 3,600 in seconds. *time*: Specifies the date and time for starting periodical notification in *yyyy-mm-ddThh:mm:ss* format.
Command Mode	CWMP configuration mode
Defaults	The default value is 600 seconds.
Usage Guide	Use this command to configure the periodic notification function of the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

- (Optional) The CPE can download firmware and configuration files from the ACS by default.
- Perform this configuration if the CPE does not need to download firmware and configuration files from the ACS.

Command	**disable download**
Parameter Description	N/A
Defaults	The CPE can download firmware and configuration files from the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of downloading main program and configuration files from the ACS. ● This command does not act on configuration script files. The configuration scripts can still be executed even if this function is disabled.

Disabling the Function of Uploading Configuration and Log Files to the ACS

- (Optional.) The CPE can upload configuration and log files to the ACS by default.

- Perform this configuration if the CPE does not need to upload configuration and log files to the ACS.

Command	**disable upload**
Parameter Description	N/A
Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

Configuring the Backup and Restoration of the Firmware and Configuration Files of the CPE

- (Optional) The backup and restoration of the firmware and configuration files of the CPE is enabled by default. The value range is from 30 to 10,000 in seconds. The default value is 60 seconds.
- The longer the delay-time is, the longer the reboot will be complete.
- Perform this configuration to modify the function of backing up and restoring the firmware and configuration files of the CPE.

Command	**cpe back-up** [**delay-time** *seconds*]
Parameter Description	*seconds*: Specifies the delay for backup and restoration of the firmware and configuration file of the CPE.
Defaults	The default value is 60 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Response Timeout

- (Optional) The value range is from 5 to 600 in seconds. The default value is 5 seconds.
- Perform this configuration to modify the ACS response timeout period on the CPE.

Command	**timer cpe- timeout** *seconds*
Parameter Description	*seconds*: Specifies the timeout period in seconds. The value range is from 5 to 600.
Defaults	The default value is 5 seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Verification

- Run the show cwmp configuration command.

Command	**show cwmp configuration**
Parameter	N/A

Description	
Command Mode	Privileged EXEC mode
Usage Guide	N/A
Configuration Examples	The following example displays the CWMP configuration. Ruijie(config-cwmp)#show cwmp configuration CWMP Status : enable ACS URL : http://www.ruijie.com.cn/acs ACS username : admin ACS password : ****** CPE URL : http://10.10.10.2:7547/ CPE username : ruijie CPE password : ****** CPE inform status : disable CPE inform interval : 60s CPE inform start time : 0:0:0 0 0 0 CPE wait timeout : 50s CPE download status : enable CPE upload status : enable CPE back up status : enable CPE back up delay time : 60s

Configuration Examples

Configuring the Periodical Notification Interval of the CPE

Network Environment	See Figure 8-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60 seconds.
CPE	Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)#cpe inform interval 60
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration CWMP Status : enable ..... CPE inform interval : 60s

Disabling the Function of Downloading Firmware and Configuration Files from the ACS

Network Environment	See Figure 8-6.
Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the function of downloading firmware and configuration files from the ACS.
CPE	Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)#disable download
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration CWMP Status : enable ..... CPE download status : disable

Disabling the Function of Uploading Configuration and Log Files to the ACS

Network Environment	See Figure 8-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Disable the CPE's function of uploading configuration and log files to the ACS.
CPE	Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)# disable upload
Verification	Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration CWMP Status : enable ..... CPE upload status : disable

Configuring the Backup and Restoration Delay

Network Environment	See Figure 8-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the backup and restoration delay to 100 seconds.

CPE	Ruijie#config Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)#cwmp Ruijie(config-cwmp)# cpe back-up Seconds 30
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie #show cwmp configuration CWMP Status : enable ..... CPE back up delay time : 30s

↘ Configuring the ACS Response Timeout of the CPE

Network Environment	See Figure 8-6.
Configuration Steps	● Enable the CWMP function and enter CWMP configuration mode. ● Set the response timeout of the CPE to 100 seconds.
CPE	Ruijie# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Ruijie(config)# cwmp Ruijie(config-cwmp)# timer cpe-timeout 100
Verification	● Run the **show** command on the CPE to check whether the configuration commands have been successfully applied.
CPE	Ruijie#show cwmp configuration CWMP Status : enable ..... CPE wait timeout : 100s

Common Errors

N/A

8.5 Monitoring

Displaying

Command	Function
show cwmp configuration	Displays the CWMP configuration.
show cwmp status	Displays the CWMP running status.

9 Configuring LED

9.1 Overview

Light Emitting Diode (LED) is a solid luminous semiconductor. It serves as an indicator light to show AP's working status in different colors.

The following part only introduces LED.

Protocols and Standards

N/A

9.2 Application

N/A

9.3 Features

Ruijie products support one or multiple LEDs to display AP's working status. For example, the LED on an Ethernet interface blink when there comes the data flow. It is controlled through GPIO or CPLD ports with different lighting, such as solid green, blinking green, blinking red and so on. By observing the LED, you can easily tell AP's working status and faults.

9.4 Configuration

Configuration Item	Configuration Suggestion & Relevant Command	
Configuring AP location.	(Optional) It is used to locate an AP.	
	led on [**slot** *slot-id*]	Turn on the LED to locate an AP. *slot-id:* Slot ID corresponding to the RF card
Configuring Quiet Mode.	(Optional). It is used to enable LED quiet mode.	
	quiet-mode session	Enable LED quiet mode.

9.4.1 Configuring AP Location

Configuration Effect

- Turn on LEDs for AP location.

Notes

- Disable the configuration after location or the lighting of LEDs no longer changes.

Configuration Method

Configuring AP Location

- Optional configuration.
- Enable this configuration before AP location, and disable it after that.

Command	**led on** [**slot** *slot-id* [**secondary**]]
Parameter Description	*slot-id*: Slot ID corresponding to the RF card. **secondary**: Applies to the secondary device.
Defaults	This function is disabled by default.
Configuration Mode	AP configuration mode
Usage Guide	For rack APs, specify the slot ID for every RF card. For non-rack APs, the *slot-id* parameter is invalid. The **secondary** parameter indicates that the command applies to the secondary device.

Check Method

- Check whether the location LED is on the AP.

Configuration Examples

Locating AP 00d0.f822.33bc

Scenario	N/A
Configuration Steps	Configure AP location on the AC.
AC	`Ruijie# configure terminal` `Ruijie(config)# ap-config 00d0.f822.33bc` `Ruijie(ap-config)# led on`
Verification	Check whether the location LED is on the AP.

Common Mistakes

N/A

9.4.2 Configuring Quiet Mode

Configuration Effect

- All LEDs on an AP are off when this command takes effect.

Notes

- You must configure the effective time for the quiet mode at first.

Configuration Method

Configuring session

- Optional configuration.
- Create a session before the configuration of the quiet mode.
- Configure the effective time for the session.

Command	**schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*
Parameter Description	*sid*: scheduled session ID. *n*: scheduled session period No. *day1*: scheduled session period; day 1indicates the start date, in the range of { sun | mon | tue | wed | thu | fri | sat }. **to** *day2*: the end date, only one day of the interval by default. **time** *hh1:mm1* **to** *hh2:mm2*: scheduled session time. hh1:mm1 is the start time and hh2:mm2 the end time in the range from 0 to 23 hours and 0 to 59 minutes.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Configure a session at first.

Configuring Quiet Mode

- Optional configuration.
- Configuring LED quiet mode.

Command	**quiet-mode session** *session-num*
Parameter Description	session-num: specifies the session ID.
Default Configuration	This function is disabled by default.
Configuration Mode	AP configuration mode
Usage Guide	Configure a session at first.

Check Method

- All LEDs are off when the system time is within the session interval.

Configuration Examples

Configuring LED Quiet Mode from Monday 11pm to Tuesday 7am Every Week

Configuration Steps	• Configure a session. • The following example configures the session ID for the quiet mode.

	Ruijie# configure terminal Ruijie(config)#schedule session 1 Ruijie(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00 Ruijie(config)#ap-config 00d0.f822.33bc Ruijie(config-ap)#quiet-mode session 1
Verification	When the system time is within the session interval, all LEDs on the AP are off.

Common Mistakes

- Configured session ID does not exist.

9.5 Monitoring

N/A

10 Configuring Software Authorization Management

10.1 Overview

Software authorization is an intermediate link for users to use some extension functions of the device. A user can use the extension functions after installing correct license files. The extension functions provided by RGOS include the VSD, TRILL, FCoE, number of users supported by the AP, and number of concurrent users supported by SSLVPN. A user can use general functions and extension functions of the RGOS after being authorized.

- Generally, all features of the RGOS are installed for the device before delivery of the device. However, users cannot use some features of the RGOS before they obtain a corresponding license file.
- Whether a feature requires authorization and the authorization type are specified in the configuration guide of the feature. Unless otherwise specified, basic functions of the system can be used without authorization.

10.2 Typical Application

10.2.1 VSD

Application Scenario

VSD is a network system virtualization technology. It is used to divide one physical device into multiple logical devices by means of virtualization. In addition, VSD makes use of existing resources to the maximum extent, reducing the network operation cost.

Before being authorized, a user can only use VSD0 (that is, common CLI). After being authorized, the user can create other VSDs.

Function Deployment

The authorization module only functions on VSD0. License files cannot be installed on other VSDs.

10.2.2 FCoE

Application Scenario

The FCoE technology can map the fiber channel to the Ethernet and insert the fiber channel information into the Ethernet information packet to enable SAN data transmission over the Ethernet instead of over the fiber channel connecting the server to the SAN storage device.

Before the FCoE license file is installed on the device, the FCoE is not available. After the FCoE license file is installed, users can use the FCoE.

Function Deployment

-

10.3 Function Details

Basic Concept

License File for a Feature

A license for a certain special feature obtained by means of license file, hardware entity, or legal contract. This license stipulates the maximum number of users allowed to use it, the maximum number of instances allowed to be used, and validity period.

Authorized Software

Software function that can be used after being authorized.

Host Number

Unique serial number for identifying each device.

⚠ In VSU environment, a license can adopt the host ID of any chassis. When the chassis exits the VSU environment, the feature corresponding to the license becomes invalid.

Authorization by Products

One license file is applied to only one device, which matches the host number. License file migration is not supported.

Purchase Voucher

Purchase voucher of a license file. This voucher contains the product activation key (PAK) and the website for downloading the license file.

Product Activation Key (PAK)

The legal owner of the purchase voucher logs in to the website (listed on the purchase voucher) for downloading the license file and uses the PAK for registration. After that, a corresponding license file is provided on the webpage for downloading or directly sent to the registered mailbox.

License File

After a license file is installed on a device, users can use relevant functions. Each license file contains a digital signature to avoid manipulation. A license file is used for authorization based on products.

License Stacking

Different license files can be used on one device. For example, if a device provides both the FCoE and TRILL functions, users can purchase the license files of the two functions and use them on the same device.

Temporary License File

A temporary license file becomes invalid after a period of time.

Evaluation License File

Evaluation license file belongs to temporary license file. Generally, an evaluation license file is installed on a device before delivery, and it is mainly used to provide users with the function of using a certain trial feature. This type of license file is independent of the host number.

Permanent License File

A permanent license file is permanently valid.

Single-Instance License File

Only one license file can be installed for a feature at a time.

⚠ Currently, the license file for the feature like the number of concurrent users supported by VSD, TRILL, FCoE, and SSLVPN is a single-instance license file.

Multi-Instance License File

Multiple license files can be installed for the same feature on a device.

⚠ Currently, only the license file for the feature "number of users supported by the AP" is a multi-instance license file.

Friendly Period Warning

Friendly period warning is issued in log or TRAP form several days before the license file expires. Friendly period warning is set to prevent a license file with a validity period from stopping working suddenly when the validity period expires, ensuring network performance.

Functions and Features

Function and Feature	Description
Obtaining and Using a License File	Describe how to obtain and use a license file.
Backing Up, Updating, and Removing a License File	Describe how to back up, update, and remove a license file.

10.3.1 Obtaining and Using a License File

Using the License File

A license file must be purchased from the website or marketing channel of Ruijie for formal authorization. Authorization is based on each device. To obtain a license file, visit the website on the purchase voucher and provide the PAK and host ID. The license file can be directly downloaded by a user or sent to a user by email. After obtaining the license file, users need to install the license file. After installing the license file, users can use the features corresponding to the license file.

The license files of the RGOS include permanent license file and temporary license file (evaluation license file is a type of temporary license file). Once a user starts using a temporary license for a certain feature, timekeeping is started for this

license file, and this feature is disabled after the validity period of the license file expires. To continue using this feature, this user can purchase another license file (permanent or temporary license file) from the website or marketing channel of Ruijie.

In the VSU environment, multiple devices form one virtual device. In this scenario, as long as one device obtains the license file for a certain feature, the VSU obtains the license file for this feature. However, when these devices are used separately again, authorization is still based on each device.

The VSD function provided by RGOS helps to divide one RGOS device into multiple virtual devices. For users, each virtual device seems like an independent device. In this environment, license files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively. Check of the License File

After a device starts to run, the license file for each authorized feature needs to be checked. If the corresponding license file is properly installed, this feature is ready for application. Otherwise, this feature becomes invalid and cannot be used.

Checking the license files for various features occurs at different times. That is, the license files for some features are checked during startup, and the license files for some features are checked in real time.

Loss of the License File

License files are stored in the **data** directory of a device and will not be lost after software upgrade.

If the memory or file system is damaged with the license file backed up, you can install the backup license file again after system recovery. If the license file is not backed up, you can visit the authorization website of Ruijie and obtain the license file again. The process of regaining the license file is the same as the process of obtaining a new license file (you do not need to purchase the license file again).

Authorization is based on each device. After a license file is provided for a specified device, authorization via this license file can be conducted on this device exclusively. The host ID may change during device maintenance or replacement. In case of host ID change, the license file obtained before can no longer be identified. In this case, contact the after-sales engineers of Ruijie.

10.3.2 Backing Up, Updating, and Removing a License File

Backing Up a License File

In case that a fault such as file system storage media damage occurs on a device, the license file on this device may be lost after you rectify this fault. Therefore, you need to back up the license file for reinstallation in case of a fault.

Updating a License File

If the existing license file in the system cannot meet users' requirements for a feature, users can visit the website of Ruijie to purchase a license file and then update the license file locally.

Removing a License File

If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. If the user want to use this feature again after removing its license file, t reinstall the license file. It is recommended that license files be kept properly.

10.4 Configuration Details

Configuration Item	Configuration Suggestion & Relevant Command	
Basic Functions of Software Authentication	Mandatory configuration. Installs a license file.	
	show license hostid	Obtains the host ID of the device.
	license install	Installs a license file manually.
	license auto-install	Installs a license file by auto-match.
Backing Up License File	Optional configuration. Backs up a license file.	
	license copy	Backs up a license file.
Friendly Period Warning	Optional configuration. Sets the time of issuing a warning before the validity period of a license file expires.	
	license grace-peroid	Sets a friendly period warning.
Updating License File	Optional configuration. Updates an existing license file on the device.	
	license update	Updates a license file.
Removing License File	Optional configuration. Removes an existing license file on the device.	
	license uninstall	Removes a license file manually.
	license auto-uninstall	Removes a license file by auto-match.
Unbinding License	Optional configuration. Unbinds the license on the device.	
	license unbind	Unbinds the license.

10.4.1 Basic Functions of Software Authorization

Configuration Effect

A license file is installed to enable the corresponding function.

Notes

- After downloading a license file from a specified website, upload this license file to the device (or store it in a USB flash drive) for installation. You don't need to connect the device to the Internet during the installation.
- Different devices cannot share the same license file.
- After a license file is installed on a device, this license file is automatically backed up in the **data** directory of the system (the name of a license file ends with ".lic"). When you remove a license file, the backup file of this license file is also removed.

Configuration Steps

Obtaining Host ID of the Device

- Mandatory configuration.
- host-id indicates the host ID.
- If you want to apply a feature requiring authorization without installing the license file, the CLI displays a prompt indicating that the unauthorized feature is unavailable and provides the website for downloading the license file.

Command	**show license hostid**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	The name of a license file cannot be modified. This command does not require license.

Obtaining the PAK

- Mandatory configuration.
- Generally, a PAK is provided in a paper purchase voucher by Ruijie after a user purchases a license file.

Obtaining the License File of the Product from Ruijie Web URL

- Mandatory configuration.
- After logging in to the authorization website, you can obtain the license file according to the prompts.

Copying the License File to the File System of the Device

- Mandatory configuration.
- Use conventional file system operation commands to perform this operation. For example, download the license file through the TFTP protocol or copy the license file to a USB flash drive.

Installing the License File

- Optional. You can use the **license-install** or **license auto-install** command to install a license file. If you use the **license install** command in the VSU environment on the supervisor module, all devices in VSU are installed with the license file. For the non-supervisor module, only the device configured with the command is installed with the license file. If you use the **license auto-install** command in VSU environment, all devices are installed with the license file by auto-match. The two commands take the same effect in the non-VSU environment.

If you use the **license install** command in the VSU environment, the whole VSU is configured with the feature corresponding to the license file as long as one device obtains that feature. Once the devices are separated, the license takes effect on only the device configured with the command.

The **license auto-install** command enables the auto-match function only in the VSU environment, In other environment, it takes the same effect as the license install command, In the VSD environment, license files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively.

Command	**license install** { **flash: | usb0:** } *filename*
Parameter Description	**flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**license auto-install** { **flash: | usb0:** } *filename*
Parameter Description	**flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the **show license all_license** command to check the license name in a non-VSU environment. If the license name is displayed, the corresponding license file is installed.
- You can run the **show license dev_license** command to check the license name in a VSU environment. If the license name is displayed, the corresponding license file is installed.

Command	**show license** { **all_license	file** [*license*] }
Parameter Description	**all_license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name.
Verification	Ruijie#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Command	**show license dev-license**
Parameter Description	**dev-license**: Displays all license files in all environments.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name.
Verification	Ruijie#show license dev-license Searching license in the system... Dev 1 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

	Dev 2 1. Service name: LIC-AP-64 Attribute: Multiple_instance, Releasable [Permanent licenses] [Licensed serial number] 19880966.lic LIC-AP-6400000012264966 19880988.lic LIC-AP-6400000012264988 [Temporary license] [Licensed serial number] 19880900.lic LIC-AP-6400000012264900 (63 days left)

Configuration Examples

Installing a VSD License File in non-VSU environment

Network Environment	To enable the VSD function
Configuration Steps	● Run the **show license hostid** command to obtain the host ID of the device. ● Register at the authorization website, and perform operation based on the prompts to obtain the license file vsd.lic for the VSD feature (the host ID of the device and PAK are required). The detailed operation is omitted in this example. ● Store the vsd.lic file in a USB flash drive, and connect the USB flash drive to the device. ● Install the vsd.lic file.
	Ruijie#show license hostid 8708EH5F00042 Ruijie#license install usb0:vsd.lic License file install success, service name: LIC-VSD.
Verification	Run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed..
	Ruijie(config)#show license all-license Searching license in the system... 1.Service name: LIC-VSD Attribute: Temporary, Single instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Installing an FC License File in VSU environment

Network Environment	To enable the FC function.
Configuration Steps	● Run the **show license** *dev-hostid* command to obtain the host ID of device 2. ● Register at the authorization website, and perform operation based on the prompts to obtain the license file fc.lic for the FC feature (the host ID of the device and PAK are required). ● Store the fc.lic file in a USB flash drive, and connect the USB flash drive to the device. ● Install the fc.lic file.
	Ruijie#show license dev-hostid Dev 1: 8708EH5F00042 Dev 2: GH3002893D300 Ruijie#license auto-install usb0:fc.lic License file install success, dev 2 installed it, service name: LIC-FC-BLADE-S.
Verification	Run the **show license dev-license** command to check the license name. If the license name is displayed, the corresponding license file is installed.
	Ruijie#show license dev-license Searching license in the system... Dev 1 1.Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 Dev 2 1. Service name: LIC-FC-BLADE-S Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FC-BLADE-S00000012265522

Common Errors

- Install a license file that does not belong to the present device.
- No matching device is available.
- Reinstall a license file.
- Install a license file with its later version installed in the system..

10.4.2 Backing Up License File

Configuration Effect

- The license files of one or all features in the system are backed up.

Notes

- The license file of the evaluation version must not be backed up.

- License files can be backed up only when sufficient storage space is available.

Generally, one license file occupies a space ranging from 4 KB to 10 KB.

Configuration Steps

Backing Up a License File of the System

- The backup license file is a regular file.
- When you back up all license files in the system, a tar file is generated.

Command	**license** { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]
Parameter Description	**copy-all**: Copies all permanent license files in the system. **copy-file** *filename*: Copies the *filename* license file in the system. ***filename*** can be the name of a license file already installed in the system or the name of a feature. When ***filename*** is a feature name, all license files already installed for this feature are backed up. **flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Uploading a License File to Another System for Storage

- You can use a file system management command to further save a license file to other storage devices, such as a USB flash drive.

Verification

- You can run the **dir** command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the **dir** command with the license file name in the **installed license** field of the feature with permanent authorization displayed by running the **show license all-license** command.

Command	**dir** [*filesystem*:] [*file-url*]
Parameter Description	*filesystem*: The file system URL followed by a colon. The file systems include **flash:**, **sata:**, **usb:**, **sd:, and tmp:**. *file-url*: Path name. The path starting with "/" indicates an absolute path. Otherwise, it is a relative path.
Command	Privileged EXEC mode

Mode	
Usage Guide	This command does not require license.
Verification	Ruijie#dir usb0:rg-license-lics Directory of usb0:/rg-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories 536870912 bytes total (740,687,872 bytes free)

Command	**show license** { **all-license | file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	Users can check whether a license file is installed by checking the feature name. ⚠ Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the single-instance license file backup is named after the feature.
Verification	Ruijie#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 3. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number] 19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988

Configuration Examples

Backing Up All License Files of the System

Network Environment	Back up all license files in the system and name the backup lics.tar.
Configuration Steps	● Connect a USB flash drive to the device. ● Back up all permanent license files in the USB flash drive and name the backup lics.tar.
	Ruijie#lic copy-all usb0:rg-license-lics/lics.tar Success to copy all permanent license.
Verification	● You can run the **dir** command to check whether the license file package is generated. After decompressing the package, you can check whether the backup is correct by comparing the files in the package with the license file name displayed in the **installed license** field of the feature with permanent authorization displayed by running the **show license all-license** command. ⚠ Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named after the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the internal single-instance license file backup is named after the feature. ⚠ In this example, the IDs 19881021.lic and 19881023.lic are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, users can still identify the mapping between license files and features.
	Ruijie#dir usb0:rg-license-lics Directory of usb0:/rg-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories 536870912 bytes total (740,687,872 bytes free) Ruijie#show license all-license Searching license in the system... 1. 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 3. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number]

	19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988

Common Errors

- Specify a license file or a file not in the system.
- Specify a temporary license file for backup (a temporary license file cannot be backed up).

10.4.3 Friendly Period Warning

Configuration Effect

- Before the validity period of an evaluation license file expires, a warning is issued in log mode, enabling users to take measures in advance.

Notes

- Each authorized feature should be set separately.
- This setting may be affected by device time adjustment.
- A permanent license file does not need to be configured with friendly period warning.

Configuration Steps

↘ **Configuring a Friendly Period Warning for an Authorized Feature**

Command	**license grace-peroid** *filename days*
Parameter Description	*filename*: name of the license file for a feature *days*: The period from the expiry time to the warning time,
Defaults	The default value is the smaller one between 120 and half the evaluation license file's validity period.
Command Mode	Privileged EXEC mode
Usage Guide	-

Verification

- 1: Set the expiry time of a license file to be earlier than the warning time, and the warning is displayed at regular intervals.
- 2: Run the **show license** command to check whether the time of the **Alarm starting point** filed is consistent with the setting.

Command	**show license** { **all-license | file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	Ruijie#show license file LIC-VSD Service name: LIC-VSD Attribute: Temporary, Single instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Configuration Examples

Changing the Friendly Period Warning Time

Network Environment	The temporary license file has already been installed on the device, and the friendly period warning time is set to 100 days.
Configuration Steps	● Set the friendly period warning time to 100 days.
	Ruijie#lic grace-period LIC-VSD 100 RG_LICENSE: success to set alarm starting point of license LIC-VSD.
Verification	When the validity period of the license file is shorter than 100 days, the friendly period warning is displayed at regular intervals.
	Ruijie#*Jun 18 10:06:36: %RG_LICENSE-4-LICENSE_DEADLINE_INFO: Service LIC-VSD will be disabled 80 days behind. In order to avoid the inconvenience to you, please log on website http://192.168.5.227:8080/login.jsf to get a new license.

Common Errors

- Set friendly period warning for a permanent license file.
- No license file is installed in the preset feature system.

10.4.4 Updating License File

Configuration Effect

- The license file for a feature of the system is updated. Generally, this configuration is performed to update an evaluation license file into a temporary license file.

Notes

- A formal permanent license file does not need to be updated.
- A license file cannot be updated to the earlier version.

A license file has a time filed. The value of this field is subject to the time when the license file is generated from the website. The later the time, the later the version.

Configuration Steps

Updating a License File

- You can run the **license update** command to update the license file for a feature.
- Update the license file without connecting the device to the Internet.

Command	**license update** { **flash:	usb0:** } *filename*
Parameter Description	**flash:** Specifies that the license file is installed in the internal flash file system. **usb0:** Specifies that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the **show license** command and check the **Attribute** field. If the field is displayed as Permanent, the corresponding attribute is updated.

Command	**show license** { **all-license	file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode

Usage Guide	This command does not require license.
Verification	Ruijie#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Configuration Examples

Updating the VSD License File

Network Environment	Update the temporary license file for VSD in the system to a permanent license file.
Configuration Steps	● Purchase the permanent license file vsd_perm.lic for VSD, store the vsd_perm.lic file in a USB flash drive, and connect the USB flash drive to the device. ● Update the license file for VSD.
	Ruijie#license update usb0:vsd_perm.lic License file update success, temporary license LIC-VSD changes into permanent.
Verification	● You can run the **show license** command and check the **Attribute** field. If the field is displayed as Permanent, the corresponding attribute is updated.
	Ruijie(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-VSD00000012266666

Common Errors

- Install a license file that does not belong to the present device.
- Replace the license file of the new version with the old version.
- Reinstall a license file.
- Replace the permanent license file with the temporary license file.

- Start update when the corresponding feature is not installed for the system.

10.4.5 Removing License File

Configuration Effect

- Remove the license files for one or all features in the system.

If a feature is not needed, the user can remove the license file for this feature to improve the utilization rate of various resources like the memory. After being removed, this feature becomes unavailable.

Notes

- If you remove the license file in use, the removal operation takes effect next time when the feature is enabled or restarted.
- To reinstall a license file after removing it, you need to obtain the license file. It is recommended that you back up the license file before removing it.

Configuration Steps

Removing a License File from the System

- Run the **license uninstall** command to remove a license file from the system.

Command	**license uninstall** { **all |** *license [filename]* }
Parameter Description	**all**: Remove all license files in the system. *license*: name of the license file to be removed *filename*: name of the file to be removed
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file removal does not take effect immediately. A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it. This command does not require license.

Verification

- You can run the **show license all-license** command to display the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Command	**show license** { **all-license | file** [*license*] }

Parameter Description	**all-license**: Displays all license files already installed on the device. **file** *filename*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	Ruijie#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889

Removing a License File in VSU environment

- Run the **license auto-uninstall** to remove a license file in VSU environment.

Command	**license auto-uninstall** *devid license* [*filename*]
Parameter Description	*devid*: The ID of the device where the file is. *license*: The name of the license to be removed. *filename*: The name of the file to be removed..
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file removal does not take effect immediately. A license file cannot be restored after it is removed. It is recommended that you back up the license file before removing it. This command does not require license.

Verification

- Run the **show license dev-license** command to display the **Service name** field. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Command	**show license dev-license**
Parameter Description	**dev-license:** Displays all license files in all environments.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.
Verification	Ruijie#show license dev-license Searching license in the system...

	Dev 1 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 Dev 2 There's no license installed in this device.

Configuration Examples

Removing the VSD License File

Network Environment	Remove the license file for VSD in the system.
Configuration Steps	● Remove the license file for the VSD feature.
	Ruijie(config)#license uninstall LIC-VSD License file uninstall LIC-VSD success.
Verification	● Run the **show license all-license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.
	Ruijie(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single instance, Releasable Licensed serial number: LIC-FCOE00000012268889
Configuration Steps	Remove the license file for the FC feature on device 2.
	Ruijie#license auto-uninstall 2 LIC-FC-BLADE-S License file uninstall LIC-FC-BLADE-S of device 2 success.
Verification	Run the **show license dev-license** command to display the **Service name** field. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.
	Ruijie#show license dev-license Searching license in the system... Dev 1 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable

	Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 Dev 2 There's no license installed in this device.

Common Errors

- The license file has not been installed on the device.
- Specify a license file not on the device.
- Uninstall a license file for a single-instance feature.

10.4.6 Unbinding License

Configuration Effect

- Unbind and inactivate a license file.

If you want to unbind a license file on the device, you should unbind the license code on the device first.

Notes

- After the license file is unbound from the device, you will get a verification code, which will be used for the unbinding operation on the authorization website.
- After the license code is unbound, the corresponding license file cannot be installed again.

Configuration Steps

Unbinding a License File

- Run the **license unbind** command to unbind a license file.

Command	**license unbind** *pak*
Parameter Description	*pak*: The license code.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run the **show license all-license** to display the installed license code. This command does not require license.

Verification

- Run the **show license all-license** command to display the **licensed serial number** field. If the license code is not displayed, it indicates that the license is unbound.

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files already installed on the device. file filename: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require license.

Configuration Example

↘ Unbinding License code LIC-VSD00000012268888

Network Environment	The license corresponding to license code LIC-VSD00000012268888 is installed.
Configuration Steps	↘ Unbind license code LIC-VSD00000012268888
	Ruijie#license unbind LIC-VSD00000012268888 Success to unbind license LIC-VSD00000012268888. The verification string is: 775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855
Verification	↘ Run the **show license all-license** command to display the **licensed serial number** field. If the license code is not displayed, it indicates that the license is unbound.
	Before Binding Ruijie#show license all-license Searching license in the system... 1. Service name: LIC-AP-64 Attribute: Releasable [Permanent licenses] [Licensed serial number] 19880966.lic LIC-AP-6400000012264966 19880988.lic LIC-AP-6400000012264988 [Temporary license] [Licensed serial number] 19880900.lic LIC-AP-6400000012264900 (63 days left) 2. Service name: LIC-VSD Attribute: Permanent, Releasable Licensed serial number: LIC-VSD00000012268888 After Binding Ruijie#show license all-license

```
Searching license in the system...
 1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]     [Licensed serial number]
    19880966.lic             LIC-AP-6400000012264966
    19880988.lic             LIC-AP-6400000012264988

    [Temporary license]      [Licensed serial number]
    19880900.lic             LIC-AP-6400000012264900
    (63 days left)
```

Common Errors

10.5 No matching license code exists on the system.Monitoring and Maintenance

Verifying the License File Configuration

Function	Command
Displays the license configuration.	**show license** { **all_license | file** *[license]*}
Displays the license configuration of all devices.	**show license dev-license**
Displays the license in use.	**show license usage**
Displays the serial number of the device where the license is installed.	**show license hostid**
Displays the host ID for the license (all devices).	**show license dev-hostid**
Displays the unbound license code on the current device.	**show license unbind-code**
Displays the unbound license code on all devices in the system.	**show license dev-unbind-code**

11 Configuring USB

11.1 Overview

Universal serial bus (USB) is an external bus standard. In this document, USB refers to a USB-compliant peripheral device, for example, a USB flash drive.

USB is a hot swappable device. You can use it to copy files (such as configuration and log files) from a communication device, or copy external data (such as system upgrade files) to the flash of the communication device.

Specific application scenarios of the USB are detailed in configuration guides of related functions. This document describes only how to identify, use, and remove the USB and view information about the USB.

11.2 Applications

Application	Description
Using a USB Flash Drive to Upgrade a Device	Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version.

11.2.1 Using a USB Flash Drive to Upgrade a Device

Scenario

Upgrade files are stored on a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version. An example of the upgrade command is as follows:

upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin

If the file is valid and execution of this command succeeds, the device will be automatically reset and run the upgraded version.

Deployment

- Use the prefix "usb0:/" to access USB 0. Run the **show usb** command to display information about the USB with the ID 0.
- Run the **upgrade** command to perform upgrade.

11.3 Features

Using the USB

Insert a USB into the USB slot. The system automatically searches for the USB. After the USB is located, the driver module automatically initializes the driver of the USB. After initialization, the system automatically loads the file system on the USB. Later, the system can read or write this USB.

- If the system finds a USB and successfully loads the driver, the following information will be displayed:

```
*Jan  1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!
*Jan  1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0(type:FAT32),size : 1050673152B(1002MB)
```

"Mass Storage" indicates the name of the searched device, and "usb0:" indicates the first USB. "Size" indicates the size of the partition. For example, according to the preceding information displayed, the USB flash drive has a space of 1002 MB.

Removing the USB

Use a command line interface (CLI) command to remove the USB first; otherwise, an error may occur if the system is currently using the USB.

- If the USB is successfully removed, the following information will be displayed:

```
OK, now you can pull out the device 0.
```

You can remove the USB only after the preceding information is displayed.

11.4 Configuration

Configuration	Description and Command	
Using a USB	Mandatory.	
	N/A	
Removing a USB	(Mandatory) It is used to remove a USB.	
	usb remove	Removes a USB.

11.4.1 Using a USB

Configuration Effect

After a USB is loaded, you can run the file system commands (such as **dir**, **copy**, and **del**) to perform operations on the USB.

Notes

- The Ruijie General Operating System (RGOS) is applicable only to devices (generally common USB flash drives) that support standard Small Computer System Interface (SCSI) commands. Other devices, such as the USB flash drive embedded in the USB network interface card (NIC) and USB flash drive with the virtual CD-ROM drive, cannot be used in the RGOS. Some devices are configured with the function of converting a USB port to the serial port.
- The USB supports only the FAT file system. Other file systems on the USB must be formatted to the FAT file system on a PC before the USB can be used on a device.
- The RGOS supports the hub. When a USB flash drive is inserted to a port on a hub, the access path becomes different. If the USB flash drive is inserted to a USB port on a device, the access path is **usbX:/**, where **X** indicates the device ID. You can run the **show usb** command to display this path. If the USB flash drive is inserted to a USB port through a hub, the access path is **usbX-Y:/**, where **X** indicates the device ID, and **Y** indicates the hub port ID. For example, **usb0-3:/** indicates port 3 on the hub that is connected to USB port 0 on the device.

Configuration Steps

Identifying a USB

A USB can be directly inserted to the USB slot without a CLI operation.

Using a USB

Perform the following operations to copy files from a USB to the flash:

- Run the **cd** command to enter the partition of the USB.
- Run the **copy** command to copy files on the USB to the flash on the device.
- Run the **dir** command to check whether the files are copied to the device.

If the USB has multiple partitions, you can access only the first FAT partition on the device.

The path of the USB does not contain any upper-level directory. After running the **cd usbX:** command to access a USB, you can run the **cd flash:** command to return to the flash file system.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Configuration Example

Using a USB Flash Drive

Scenario	Standalone environment
Configuration Steps	• Insert the USB flash drive into the USB slot of the device. • Run the **show usb** command on the device console. • Copy the **config.txt** file from the USB flash drive to the flash on the device.
	`Ruijie#show usb` `Device: Mass Storage`

```
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789686784B(15789.6MB)
Ruijie#
Ruijie#
Ruijie#dir usb0:/
Directory of usb0:/
   1 -rwx             4  Tue Jan  1 00:00:00 1980  fac_test
   2 -rwx             1  Mon Sep 30 13:15:48 2013  config.txt
2 files, 0 directories
15,789,711,360 bytes total (15,789,686,784 bytes free)
Ruijie#
Ruijie#
Ruijie#copy usb0:/config.txt flash:/
Copying: !
Accessing usb0:/config.txt finished, 1 bytes prepared
Flushing data to flash:/config.txt...
Flush data done
Ruijie#
Ruijie#
```

Verification	● Check whether the **config.txt** file exists on the flash.

```
Ruijie#
Ruijie#dir flash:/
Directory of flash:/
   1 drw-           160  Wed Mar 31 08:40:01 2010  at
   2 drwx           160  Thu Jan  1 00:00:11 1970  dm
   3 drwx           160  Thu Jan  1 00:00:05 1970  rep
   4 drwx           160  Mon Apr 26 03:42:00 2010  scc
```

```
  5 drwx           160  Wed Mar 31 08:39:52 2010  ssh
  6 drwx           224  Thu Jan  1 00:00:06 1970  var
  7 d---           288  Sat May 29 06:07:45 2010  web
  8 drwx           160  Thu Jan  1 00:00:11 1970  addr
  9 drwx           160  Sat May 29 06:07:44 2010  cwmp
 10 drwx           784  Sat May 29 06:07:47 2010  sync
 11 --w-            92  Tue Feb  2 01:06:55 2010  config_vsu.dat
 12 -rw-           244  Sat Apr  3 04:56:52 2010  config.text
 13 -rwx             1  Thu Jan  1 00:00:30 1970  .issu_state
 14 -rw-             0  Tue Feb  2 01:07:03 2010  ss_ds_debug.txt
 15 -rw-          8448  Thu Jan  1 00:01:41 1970  .shadow
 16 -rwx           268  Thu Jan  1 00:01:41 1970  .pswdinfo
 17 -rw-             4  Tue May 25 09:12:01 2010  reload
 18 drwx           232  Wed Mar 31 08:40:00 2010  snpv4
 19 drwx          6104  Sat May 29 06:10:45 2010  .config
 20 ----             1  Thu Jan  1 00:04:51 1970  config.txt
 21 d---           160  Thu Jan  1 00:00:12 1970  syslog
 22 drwx           160  Tue May 25 03:05:01 2010  upgrade_ram
 23 drwx           160  Tue Feb  2 01:06:54 2010  dm_vdu
 24 -rwx            16  Thu Jan  1 00:01:41 1970  .username.data
9 files, 15 directories
5,095,424 bytes total (4,960,256 bytes free)
Ruijie#
```

Common Errors

- Insert a USB flash drive that supports non-SCSI commands to the device.
- The USB does not use the FAT file system, and cannot be identified by the system.

11.4.2 Removing a USB

Configuration Effect

Remove the USB and ensure that the USB and the device are intact.

Notes

- Run the **usb remove** command before removing the USB; otherwise, a system error occurs.

Configuration Steps

Running the Remove Command

- Mandatory.
- Run the **usb remove** command before removing the USB.

Removing the USB

After the remove command is executed, remove the USB.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Related Commands

Removing a USB

Command	**usb remove** *device-id*
Parameter Description	*device-id*: Indicates the ID of the USB port on the device. You can run the **show usb** command to display this ID.
Command Mode	Privileged EXEC mode
Usage Guide	Before removing a USB, run the **usb remove** command; otherwise, an error occurs if the USB is in use. If the command is executed, related information will be displayed, and you can remove the USB. If the command execution fails, the USB is in use. In this case, do not remove the USB until it is not in use.

Configuration Example

Removing a USB

Scenario	Standalone environment
Configuration Steps	• Run the **show usb** command to display the ID of the USB. • Run the **usb remove** command to remove the USB.
	Ruijie#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0(type:vfat)

	Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) Ruijie# Ruijie# Ruijie#usb remove 0 OK, now you can pull out the device 0.
Verification	● Run the **show usb** command again to check whether the USB is removed. If the device with ID 0 is not displayed in output of the **show usb** command, the USB is removed.
	Ruijie#show usb Ruijie#

11.5 Monitoring

Displaying

Description	Command
Displays information about the inserted USB.	**show usb**

12 Configuring PKG_MGMT

12.1 Overview

Package management (pkg_mgmt) is a package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying and maintaining various components of the device, among which upgrade is the main function. Through upgrade, users can install new version of software that is more stable or powerful. Adopting a modular structure, the RGOS system not only supports overall upgrade and subsystem upgrade but also supports separate upgrade of a feature package. In addition, the RGOS system supports upgrade through hot patches.

Component upgrade described in this document applies to both the box-type device and rack-type device. In addition, this document is for only version 11.0 and later, excluding those upgraded from earlier versions.

Protocols and Standards

N/A

12.2 Applications

Application	Scenario
Upgrading/Degrading Subsystem	Upgrade subsystem firmware like boot, kernel, and rootfs on the box-type device and rack-type device.
Upgrading/Degrading a Single Feature Package	Upgrade a single feature package on the box-type device and rack-mount device.
Installing a Hot Patch Package	Install a hot patch, and repair a certain part of the feature component.

12.2.1 Upgrading/Degrading Subsystem

Scenario

After the upgrade of a subsystem firmware is complete, all system software on the device is updated, and the overall software is enhanced. Generally, the subsystem firmware of the box-type device is called main package.

The main features of this upgrade mode are as follows: All software on the device is updated after the upgrade is completed; all known software bugs are fixed. It takes a long time to finish upgrade.

Deployment

You can store the main package in the root directory of the TFTP server, download the package to the device, and then run an upgrade command to upgrade the package locally. You can also store the main package in a USB flash drive, connect the USB flash drive to the device, and then run an upgrade command to upgrade the package.

12.2.2 Upgrading/Degrading a Single Feature Package

Scenario

Device software consists of several components, and each component is an independent feature module. After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced with the other features unchanged.

The features of this upgrade mode are as follows: Generally, a feature package is small and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

12.2.3 Installing a Hot Patch Package

Scenario

To fix software bugs without restarting the device, you can install hot patch packages. Hot patch packages are only applicable to fixing a specific software version. Generally, hot patch packages are released to fix the software of a certain version only when the device cannot be started in the user's environment.

The most significant feature of hot patch upgrade is that all bugs can be fixed without device restart after the upgrade is completed.

Deployment

You can store this package in the root directory of the TFTP server, download the package to the local device, and then complete the upgrade. You can also store the package in a USB flash drive, connect the USB flash drive to the device, and then complete the upgrade.

12.3 Features

Basic Concepts

↘ Subsystem

A subsystem exists on a device in the form of images. The subsystems of the RGOS include:

- boot: After being powered on, the device loads and runs the boot subsystem first. This subsystem is responsible for initializing the device, and loading and running system images.
- kernel: kernel is the OS core part of the system. This subsystem shields hardware composition of the system and provides applications with abstract running environment.

- rootfs: rootfs is the collection of applications in the system.

Main Package

- Main package is often used to upgrade/degrade a subsystem of the box-type device. The main package is a combination package of the boot, kernel, and rootfs subsystems. The main package can be used for overall system upgrade/degradation.

Feature Package of RGOS

- The feature package of RGOS refers to a collection which enables a certain feature. When the device is delivered, all supported functions are contained in the rootfs subsystem. You can upgrade only a specific feature by upgrading a single feature package.

Hot Patch Package

- A hot patch package contains the hot patches of several features. You can upgrade a hot patch package to install patches for various features. New features are provided immediately without device restart after the upgrade.

"Firmware" in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description
Upgrading/Degrading and Managing Subsystem Components	Upgrades/degrades a subsystem.
Upgrading/Degrading and Managing Functional Components	Upgrades/degrades a functional component.
Upgrading/Degrading and Managing Hot Patch Packages	Installs a hot patch package.

12.3.1 Upgrading/Degrading and Managing Subsystem Components

Subsystem upgrade/degradation aims to upgrade the software by replacing the subsystem components of the device with the subsystem components in the firmware. The subsystem component contains redundancy design. Subsystems of the device are not directly replaced with the subsystems in the package during upgrade/degradation in most cases. Instead, subsystems are added to the device and then activated during upgrade/degradation.

Working Principle

Upgrade/Degradation

Various subsystems exist on the device in different forms. Therefore, upgrade/degradation varies with different subsystems.

- boot: Generally, this subsystem exists on the norflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the norflash device.

- kernel: This subsystem exists in a specific partition in the form of files. Therefore, upgrading/degrading this subsystem is to write the file.
- rootfs: Generally, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading/degrading this subsystem is to write the image into the nandflash device.

Management

Query the subsystem components that are available currently and then load subsystem components as required.

Each subsystem component contains redundancy design. During the upgrade/degradation:

- boot: The boot subsystem always contains a master boot subsystem and a slave boot subsystem. Only the master boot subsystem is involved in the upgrade, and the slave boot subsystem serves as the redundancy backup all along.
- kernel: as the kernel subsystem contains at least one redundancy backup. More redundancy backups are allowed if there is enough space.
- rootfs: The rootfs subsystem always contains a redundancy backup.

The boot component is not included in the scope of subsystem management due to its particularity. During upgrade of the kernel or rootfs subsystem component, the upgrade/degradation module always records the subsystem component in use, the redundant subsystem component, and management information about various versions.

Relevant Configuration

Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

12.3.2 Upgrading/Degrading and Managing Functional Components

Working Principle

In fact, upgrading a feature is replacing feature files on the device with the feature files in the package.

Managing feature components and hot patches is aimed at recording the information of feature components and hot patches by using a database. In fact, installing, displaying and uninstalling a component is the result of performing the Add, Query and Delete operation on the database.

After package upgrade, component upgrade cannot be performed.

Relevant Configuration

Upgrade

- Store the upgrade file on the local device, and then run the **upgrade** command for upgrade.

12.3.3 Upgrading/Degrading and Managing Hot Patch Packages

Working Principle

In fact, upgrading a feature component is replacing feature files on the device with the feature files in the package.

Upgrading hot patch packages is similar to upgrading features. The difference is that only files to be revised are replaced during hot patch package upgrade. In addition, after the files are replaced, the new files take effect automatically.

After package upgrade, component upgrade cannot be performed.

Management

Similar to feature component management, hot patch management also includes the query, installation, and uninstallation operation, which is the result of adding, querying and deleting data respectively.

Hot patches and feature components are managed based on the same technology. The difference is that the hot patches involve three different states, that is, Not installed, Installed, and Activated. These states are described as follows:

The hot patch in Installed state only indicates that this hot patch exists on the device, but it has not taken effect yet.

Only the hot patch in Activated state is valid.

Relevant Configuration

Upgrade

- Store the upgrade file in the local file system, and then run the **upgrade** or **upgrade patch** command for upgrade.

Activating a Hot Patch

- You can run the **patch active** command to activate a patch temporarily. The patch becomes invalid after device restart. To use this patch after device restart, you need to activate it again.
- You can also run the **patch running** command to activate a patch already permanently. The patch is still valid after device start.
- The patch not activated will never become valid.

Deactivating a Hot Patch

- To deactivate an activated patch, run the **patch deactive** command.

Uninstalling a Hot Patch

- You can run the **patch delete** command to uninstall a hot patch.

12.4 Configuration

Configuration	Description and Command
Upgrading/Degrading a Firmware	The basic function of the configuration is installing and upgrading/degrading a subsystem firmware, feature package, and hot patch package. This command is valid on both the box-type device and rack-type device.

	upgrade [**patch**] *url* [**force**]	*url* is a local path where the firmware is stored. This command is used to upgrade the firmware stored on the device.
	upgrade [**patch**] **download tftp://***path* [**force**]	*path* is the path of the firmware on the server. This command is used to download a firmware from the server and upgrade the package automatically.

12.4.1 Upgrading/Degrading a Firmware

Configuration Effect

Available firmwares include the main package, rack package, various feature packages and hot patch packages.

- After the upgrade of the main package is complete, all system software on the line card is updated, and the overall software is enhanced.
- After an independent feature package is upgraded, only the feature bug corresponding to this package is fixed. Besides, this feature is enhanced, with other features remain unchanged.
- Upgrading hot patch packages is aimed at fixing software bugs without restarting the device. Hot patch packages are only applicable to fixing bugs for a specific version of software.

Generally a main package is released to upgrade a box-type device.

Notes

N/A

Configuration Steps

Upgrading the Main Package for a Single Device

- Optional configuration. This configuration is required when all system software on the device needs to be upgraded.
- Download the firmware to the local device and run the **upgrade** or **upgrade patch** command.

Generally a main package is pushed to upgrade a box-type device.

Upgrading Each Feature Package

- Optional configuration. The configuration is used to fix bugs of a certain feature and enhance the function of this feature.
- Download the firmware to the local device and run the **upgrade** command.

Upgrading a Hot Patch Package

- Optional configuration. The configuration is used to fix software bugs without restarting the device.
- Download the firmware to the local device and run the **upgrade** command.

- After being upgraded, the hot patch can be used after it is activated. The configuration in this step is mandatory. Two activation modes are available: Run the **patch active** command to activate a patch temporarily, or run the **patch running** command to activate a patch permanently.

⚠ Generally, the **patch running** command must be used to activate a patch permanently in the user scenario. The **patch active** command can be used to activate a patch only when a user intends to verify the patch.

Subsystem Rollback

- Optional configuration. This configuration aims to roll a subsystem back to the state before the upgrade, select this configuration item..
- This configuration takes effect after you run the **upgrade** command to upgrade the subsystem component (for example, the main package).

⚠ After you run the **upgrade** command to upgrade a subsystem component in the user scenario, you can run the rollback command once, that is, consecutive rollback is not supported.

Verification

- After upgrading a subsystem component, you can run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a feature component, you can run the **show component** command to check whether the upgrade is successful.
- After upgrading a hot patch package, you can run the **show patch** command to check whether the upgrade is successful.

Commands

Upgrade

Command	**upgrade** [**patch**] [**peer** { **all** | *ip-address*}] *url* [**force**]
Parameter Description	**patch**: Patch upgrade. **peer**: A peer device. **all**: All devices *ip-address*: Specifies a device **force***:* Compulsory upgrade
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**upgrade** [**patch**] **download tftp:/***path* [**force**]

	upgrade [**patch**] **download oob_tftp:**/*path* **[via mgmt** *{number}***]** [**force**] **upgrade** [**peer** { **all** | *ip-address*}] **download tftp:**/*path* [**force**]
Parameter Description	**via mgmt** *number*: If the transfer mode is *oob_tftp* and there are multiple MGMT ports, you can select a specific port. **peer**: A peer device. **all**: All devices *ip-address*: Specifies a device **force**: Compulsory upgrade
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Firmware Stored on the Device

Command	**show upgrade file** *url*
Parameter Description	*url* indicates the path of the firmware in the device file system.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Upgrade History

Command	**show upgrade history**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Subsystem Component Rollback

Command	**upgrade rollback**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to undo the last subsystem upgrade operation and make the subsystem restore to the state before the upgrade. You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Displaying the Feature Components Already Installed

Command	**show component**
Parameter Description	[*component _name*]: component name When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Upgrade Status

Command	**show upgrade peer** { **all** | *ip-address* } **status**
Parameter Description	**peer**: A peer device. **all**: All devices *ip-address*: Specifies a device
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Patch Packages Already Installed

Command	**show patch** [*package _name*]
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Activating the Patches Temporarily

Command	**patch active**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch temporarily, and the activated patch becomes invalid after device restart.

Activating the Patches Permanently

Command	patch running
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device already installed with a patch. This command can be used to activate a patch permanently.

Configuration Example

↘ Example of Upgrading a Subsystem Firmware on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, insert the USB flash drive to the device, and then run the **upgrade** *url* command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the upgrade command. ● After upgrading the subsystem, restart the device.
	Ruijie# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin... !!! !!! !!! !!! !!!!!!!!!!!!!!!! Transmission finished, file length 21525888 bytes. Upgrade processing is 10% Upgrade processing is 60% Upgrade processing is 90% Upgrade info [OK] Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f] Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8] Upgrade processing is 100% Reload system to take effect! Reload system?(Y/N)y Restarting system.

Verification	● Check the system version on the current device. If the version information changes, the upgrade is successful.
	Ruijie#show upgrade history Last Upgrade Information: Time: 2014-08-31 12:15:03 Method: LOCAL System software version : _RGOS11.0(1)B1_CM_01200616_install.bin

Example of Upgrading a Feature Package on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade** *url* command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the **upgrade** command. ● Check whether the device needs to be restarted based on the prompt displayed after the upgrade.
	Ruijie#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm Ruijie#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm Upgrade processing is 10% Upgrade processing is 60% Upgrade processing is 90% Upgrade info [OK] bridge version[2.0.1.37cd5cda ->2.3.1.1252ea] [OK] Upgrade processing is 100% Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the version of the feature component on the current device. If the version information changes, the upgrade is successful.
	Ruijie# show component Package :sysmonit Version:1.0.1.23cd34aa Build time: Wed Dec 7 00:58:56 2011 Size:12877 Install time :Wed Mar 5 14:23:12 2012

	Description:this is a system monit package Required packages: None ---------- package:bridge Version: 2.3.1.1252ea Build time: Wed Dec 7 00:54:56 2011 Size:26945 Install time : Wed Mar 19:23:15 2012 Description:this is a bridge package Required packages: None

Example of Installing a Patch Package on the Box-Type Device

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the upgrade command. ● Activate the hot patch.
	Ruijie#upgrade download tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin Accessing tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin... !!! !!! !!!!!!!!!!!!!!!! Transmission finished, file length 9868 bytes. Upgrade processing is 10% Upgrade processing is 60% Upgrade info [OK] patch_bridge version[1.0.0.1952] Upgrade processing is 90% Upgrade info [OK] patch_install version[1.0.0.192e35a] Ruijie#patch running The patch on the system now is in running status
Verification	● Check the hot patches installed on the current device.
	:patch package patch_install installed in the system, version:pa1 Package : patch_bridge

	Status: running Version: pa1 Build time: Mon May 13 09:03:07 2013 Size: 277 Install time: Tue May 21 03:07:17 2013 Description: a patch for bridge Required packages: None

Example of Subsystem Rollback on the Box-Type Device

You can perform the rollback operation only if the last upgrade is subsystem upgrade and the upgrade is successful. The rollback command cannot be executed in succession.

Network Environment	Before the upgrade, you must copy the firmware to the device. The upgrade module provides the following solutions. ● Run some file system commands like **copy tftp** and **copy xmodem** to copy the firmware on the server to the device file system, and then run the **upgrade *url*** command to upgrade the firmware in the local file system. ● Run the **upgrade download tftp://*path*** command directly to upgrade the firmware file stored on the tftp server. ● Copy the firmware to a USB flash drive, connect the USB flash drive to the device, and then run the **upgrade *url*** command to upgrade the firmware in the USB flash drive.
Configuration Steps	● Run the subsystem rollback command. ● Restart the device for the rollback to take effect.
	Ruijie#upgrade rollback kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK] rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK] Rollback success! Reload system to take effect! Reload system?(Y/N)y Restarting system.
Verification	● Check the system version on the current device. If t it is restored to the version before the upgrade, the rollback is successful.
	Ruijie#show upgrade history Last Upgrade Information: Time: 2014-08-31 12:15:03 Method: LOCAL Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin Package Type: Distribution

Common Errors

If an error occurs during the upgrade, the upgrade module displays an error message. The following provides an example:

```
Upgrade info [ERR]
       Reason:creat config file err(217)
```

The following describes several types of common error messages:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. It is recommended to obtain the firmware again and perform the upgrade operation.
- Firmware not supported by the device: The cause is that you may use the firmware of other devices by mistake. It is recommended to obtain the firmware again, verify the package, and perform the upgrade operation.
- Insufficient device space: Generally, this error occurs on a rack-type device. It is recommended to check whether the device is supplied with a USB flash drive. Generally, this device has a USB flash drive.

12.4.2 Deactivating and Uninstalling a Hot Patch

Configuration Effect

An activated hot patch is deactivated or uninstalled.

Notes

A hot patch that is not activated does not take effect; therefore, you cannot deactivate it.

Configuration Steps

Deactivating an Activated Patch

- Optional configuration. To deactivate an activated patch, run the **patch deactive** command.

Uninstalling a Hot Patch

- Optional configuration. To uninstall a hot patch already installed, run the **patch delete** command.

Verification

- You can run the **show patch** command to check whether a patch is activated or uninstalled.

Commands

Deactivating an Activated Patch

Command	**patch deactive** [**slot** { *num* **| M1 | M2 | all** }]
Parameter Description	**slot:** indicates that this command is executed on the device in the specified slot. *num*: indicates the slot number of the specified line card. **M1 and M2**: indicate the supervisor modules. **all**: indicates all devices.
Command Mode	Privileged EXEC mode
Usage Guide	You can perform this operation on only an activated patch. All parameters are applicable to only the rack-type device.

Deleting a Hot Patch

Command	**patch delete**
Parameter Description	
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to remove the hot patch package from the device.

Configuration Example

Deactivating and Uninstalling a Patch on the Box Device

Configuration Steps	● Run the patch deactivation command. ● Run the patch deletion command.
	Ruijie#patch deactive Deactive the patch package success Ruijie# patch delete Clear the patch patch_bridge success Clear the patch success
Verification	● Display patch status.
	Ruijie#show patch No patch package installed in the system

Common Errors

- Run the **patch deactive** command when the patch is not activated. It is recommended to check the patch status. You can run the **patch deactive** command only when the patch is in the **status:running** state.

12.5 Monitoring

Clearing

Function	Command
Deletes a hot patch package already installed.	**patch delete**

Displaying

Function	Command
Displays all components already installed on the current device and their information.	**show component** [*component _name*]
Displays the information about the hot patch packages already installed on the device.	**show patch** [*patch _name*]

Displays the upgrade history.	**show upgrade history**

13 Configuring NTP

13.1 Overview

The Network Time Protocol (NTP) is an application-layer protocol that enables network devices to synchronize time. NTP enables network devices to synchronize time with their servers or clock sources and provides high-precision time correction (the difference from the standard time is smaller than one millisecond in a LAN and smaller than decades of milliseconds in a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment.

Currently, Ruijie devices can be used both as NTP clients and NTP servers. In other words, a Ruijie device can synchronize time with a time server, and be used as a time server to provide time synchronization for other devices. When a Ruijie device is used as a server, it supports only the unicast server mode.

Protocols and Standards

- RFC 1305 : Network Time Protocol (Version 3)

13.2 Applications

Application	Description
Synchronizing Time Based on an External Reference Clock Source	A device is used as a client that synchronizes time with an external clock source. After successful synchronization, it is used as a server to provide time synchronization for other devices.
Synchronizing Time Based on a Local Reference Clock Source	A device uses a local clock as a reliable NTP reference clock source and is also used as a server to provide time synchronization for other devices.

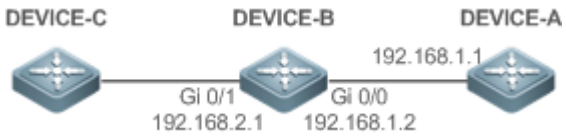
13.2.1 Synchronizing Time Based on an External Reference Clock Source

Scenario

As shown in Figure 13-1:

- DEVICE-A is used as a reliable reference clock source to provide time synchronization for external devices.
- DEVICE-B specifies DEVICE-A as the NTP server and synchronizes time with DEVICE-A.
- After successful synchronization, DEVICE-B provides time synchronization for DEVICE-C.

Figure 13-1



Deployment

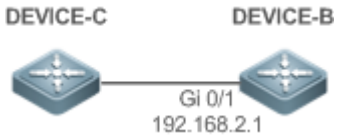
Configure DEVICE-B to the NTP external reference clock mode.

13.2.2 Synchronizing Time Based on a Local Reference Clock Source

Scenario

As shown in Figure 13-2, DEVICE-B uses a local clock as the NTP reference clock source and provides time synchronization for DEVICE-C.

Figure 13-2



Deployment

Configure DEVICE-B to the NTP local reference clock mode.

13.3 Features

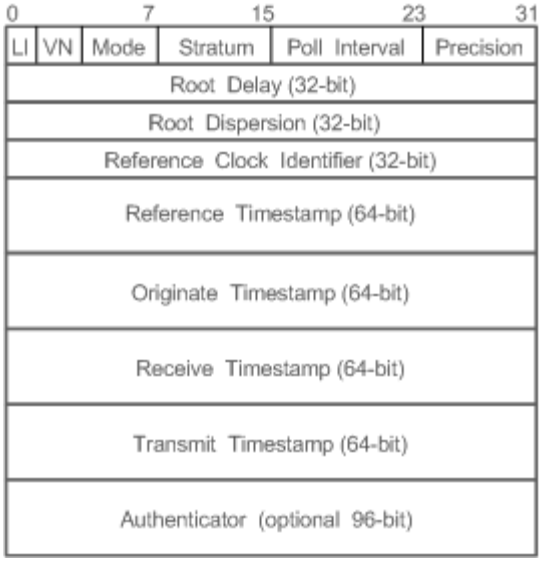
Basic Concepts

NTP Packet

As defined in RFC1305, NTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 13-3 shows the format of an NTP time synchronization packet.

Figure 13-3 Format of an NTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP version number. The current version number is 3.
- Mode: indicates a 3-bit NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master reference clock source; other values: indicate slave reference clock sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.
- Root Delay: indicates the round-trip time to the master reference clock source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

NTP Server

A device uses a local clock as the reference clock source to provide time synchronization for other devices in the network.

NTP Client

A device is used as an NTP client that synchronizes time with an NTP server in the network.

Stratum

In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratums have higher clock precisions.

Hardware Clock

A hardware clock operates based on the frequency of the quartz crystal resonator on a device and is powered by the device battery. After the device is shut down, the hardware clock continues running. After the device is started, the device obtains time information from the hardware clock as the software time of the device.

Overview

Feature	Description
NTP Time Synchronization	Network devices synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Security Authentication	The NTP packet encryption authentication is used to prevent unreliable clock sources from time synchronization interference on a device.
NTP Access Control	An Access Control List (ACL) is used to filter sources of received NTP packets.

13.3.1 NTP Time Synchronization

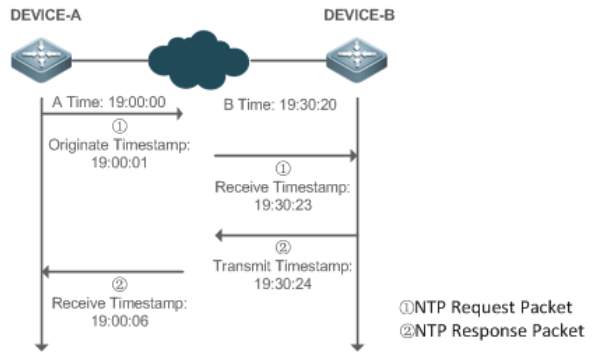
Working Principle

NTP time synchronization is implemented by interaction of NTP packets between a client and a server:

- The client sends a time synchronization packet to all servers every 64 seconds. After receiving response packets from the servers, the client filters and selects the response packets from all servers, and synchronizes time with an optimum server.
- After receiving the time synchronization request packet, a server uses the local clock as the reference source, and fills the local time information into the response packet to be sent to the client based on the protocol requirement.

Figure 13-4 shows the format of an NTP time synchronization packet.

Figure 13-4 Working Principle of NTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an NTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

1. A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
2. After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.

3. B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
4. After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

NTP Working Mode

- External clock reference mode

In this mode, a device is used as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server first and provide time synchronization for the clients after successful synchronization.

- Local clock reference mode

In this mode, a device uses the default local clock as the reliable clock source and provides time synchronization directly for other clients.

Related Configuration

Configuring an NTP Server

- The NTP function is disabled by default.
- Run the **ntp server** command to specify an NTP server (external clock reference source), which can enable NTP.
- After the configuration, the device works in the external clock reference mode.

Real-time Synchronization

- A device performs time synchronization every 64 seconds by default.

Updating a Hardware Clock

- By default, a device does not update synchronized time to the hardware clock.
- Run the **ntp update-calendar** command to enable a device to automatically update the hardware clock after successfully synchronizing time each time.

Configuring the NTP Master Clock

- By default, a device works in the external clock reference mode.
- Run the **ntp master** command to configure a device to the local clock reference mode.

13.3.2 NTP Security Authentication

To prevent malicious damage on an NTP server, NTP uses the authentication mechanism to check whether the time synchronization information is really from the announced server and check the information return path to provide an anti-interference protection mechanism.

Working Principle

An NTP client and an NTP server are configured with the same key. When sending request and response packets, a device calculates the hash values of the packets by using the MD5 algorithm based on the specified key and NTP packet content, and fills the hash values into the packet authentication information. The receiving device checks whether the packets are sent by a trusted device or modified based on the authentication information.

Related Configuration

Configuring a Global Security Authentication Mechanism for NTP

- By default, no NTP security authentication mechanism is enabled.
- Run the **ntp authenticate** command to enable the NTP security authentication mechanism.

Configuring a Global Authentication Key for NTP

- By default, no global authentication key is configured.
- Run the **ntp authentication-key** command to enable an NTP global authentication key.

Configuring a Globally Trusted Key ID for NTP

- By default, no globally trusted key is configured.
- Run the **ntp trusted-key** command to configure a device as the reference clock source to provide a trusted key for time synchronization externally.

Configuring a Trusted Key ID for an External Reference Clock Source

- Run the **ntp server** command to specify an external reference source and the trusted key of this clock source as well.

13.3.3 NTP Access Control

Working Principle

Provide a minimum security measure by using an ACL.

Related Configuration

Configuring the Access Control Rights for NTP Services

- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure the access control rights for NTP.

13.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of NTP	(Mandatory) It is used to enable NTP. After NTP is enabled, a device works in the external clock reference mode.	
	ntp server	Configures an NTP server.
	ntp update-calendar	Automatically updates a hardware clock.
	(Optional) It is used to configure a device to the local clock reference mode.	
	ntp master	Configures the NTP master clock.
	(Optional) It is used to configure the local clock reference mode for devices.	
	ntp interval	Configures the interval for time synchronization between the NTP client and the NTP server.
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables receiving of NTP packets from a specified interface.
Configuring NTP Security Authentication	(Optional) It is used to prevent unreliable clock sources from performing time synchronization interference on a device.	
	ntp authenticate	Enables a security authentication mechanism.
	ntp authentication-key	Configures a global authentication key.
	ntp trusted-key	Configures a trusted key for time synchronization.
	ntp server	Configures a trusted key for an external reference clock source.
Configuring NTP Access Control	(Optional) It is used to filter the sources of received NTP packets.	
	ntp access-group	Configures the access control rights for NTP.

13.4.1 Configuring Basic Functions of NTP

Configuration Effect

External Clock Reference Mode

- Use a device as a client to synchronize time from an external reference clock source to the local clock.

- After the time synchronization is successful, use the device as a time synchronization server to provide time synchronization.

Local Clock Reference Mode

- Use the local clock of a device as the NTP reference clock source to provide time synchronization.

Notes

- In the client/server mode, a device can be used as a time synchronization server to provide time synchronization only after successfully synchronizing time with a reliable external clock source.
- Once the local clock reference mode is configured, the system will not synchronize time with a clock source with a higher stratum.
- Configuring a local clock as the master clock (especially when specifying a lower stratum) may overwrite an effective clock source. If this command is used for multiple devices in a network, the clock difference between the devices may cause unstable time synchronization of the network.
- Before a local clock is configured as the master clock, if the system never synchronizes time with an external clock source, you may need to manually calibrate the system clock to ensure that there is no excessive difference. For details about how to manually calibrate the system clock, refer to the system time configuration section in the configuration guide.

Configuration Steps

Configuring an NTP Server

- (Mandatory) At least one external reference clock source must be specified (A maximum of 20 different external reference clock sources can be configured).
- If it is necessary to configure an NTP key, you must configure NTP security authentication before configuring the NTP server.

Configuring the Interval for Time Synchronization Between the NTP Client and the NTP Server

- The default NTP time synchronization interval is 64s.

Automatically Updating a Hardware Clock

- Optional.
- By default, the system updates only the system clock, but not the hardware clock after successful time synchronization.
- After this command is configured, the system automatically updates the hardware clock after successful time synchronization.

Configuring the NTP Master Clock

- To switch a device to the local clock reference mode, run this command.

Disabling NTP

- To disable NTP and clear NTP configurations, run the **no ntp** command.
- By default, all interfaces can receive NTP packets after NTP is enabled. To disable NTP for a specified interface, run the **ntp disable** command.

Verification

- Run the **show ntp status** command to display the NTP configuration.
- Run the **show clock** command to check whether time synchronization is completed.

Related Commands

Configuring an NTP Server

Command	**ntp server**{ *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain*}[**version** *version*][**source** *if-name*][**key** *keyid*][**prefer**]
Parameter Description	*ip-addr*: Indicates the IPv4/IPv6 address of the reference clock source. *domain*: Indicates the IPv4/IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number, ranging from 1 to 3. *if-name*: Indicates the interface type, including AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and Vlan. *keyid*: Indicates the key used for communicating with the reference clock source, ranging from 1 to 4294967295. **prefer**: Indicates whether the reference clock source has a high priority.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. Ruijie client system supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the related key) to initiate encrypted communication with the servers. ⚠ If it is necessary to configure an authentication key, you must configure NTP security authentication before configuring an NTP server. The default version of NTP for communicating with a server is NTP version 3. In addition, you can configure the source interface for transmitting NTP packets and specify that the NTP packets from a corresponding server can be received only on the transmitting interface.

Configuring the Interval for Time Synchronization Between the NTP Client and the NTP Server

Command	**ntp interval**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	The default NTP time synchronization interval is 64s.

Updating a Hardware Clock

Command	**ntp update-calendar**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Local Reference Clock Source

Command	**ntp master**[*stratum*]
Parameter Description	*stratum*: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling NTP

Command	**no ntp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command can be used to fast disable all functions of NTP and clear all NTP configurations.

Disabling Receiving of NTP Packets on an Interface

Command	**ntp disable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

External Clock Reference Mode of NTP

Scenario **Figure 13-5**	
	● DEVICE-B is configured to the NTP external clock reference mode. ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-A configures the local clock as the NTP reference clock source. ● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-A	A#configure terminal A(config)# ntp master A(config)#exit
DEVICE-B	B#configure terminal B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show ntp status** command on DEVICE-B to display the NTP configuration. ● DEVICE-B sends a time synchronization packet to 192.168.1.1 in order to synchronize time with DEVICE-A. ● After successfully synchronizing time with DEVICE-A, DEVICE-B can respond to the time synchronization request from DEVICE-C. ● Run the **show clock** command on DEVICE-B and DEVICE-C to check whether the time synchronization is successful.

↘ Local Clock Reference Mode of NTP

Scenario **Figure 13-6**	
	● DEVICE-B configures the local clock as the NTP reference clock source. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures the local clock as the NTP reference clock source.

	● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful.

13.4.2 Configuring NTP Security Authentication

Configuration Effect

Synchronizing Time from a Trusted Reference Clock Source

Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.

Providing Time Synchronization for a Trusted Device

Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

Notes

The authentication keys of the client and server must be the same.

Configuration Steps

Configuring a Global Security Authentication Mechanism for NTP

- Mandatory.
- By default, a device disables the security authentication mechanism.

Configuring a Global Authentication Key for NTP

- Mandatory.
- By default, a device is not configured with an authentication key.

Configuring a Globally Trusted Key ID for NTP

- Optional.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID.
- Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.

Configuring an Authentication Key ID for an External Reference Clock Source

- Optional.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID.
- Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.

Verification

- Run the **show run** command to verify the NTP configuration.
- Run the **show clock** command to check whether time is synchronized only with a trusted device.

Related Commands

Enabling a Security Authentication Mechanism

Command	**ntp authenticate**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]
Parameter Description	*key-id*: indicates the ID of a global authentication key, ranging from 1 to 4294967295. *key-string*: indicates a key string. *enc-type*: (optional) indicates whether an entered key is encrypted. 0 indicates no encryption, and 7 indicates simple encryption. The default setting is no encryption.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for NTP

Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key, ranging from 1 to 4294967295.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring a Trusted Key for an External Reference Clock Source

Refer to the section "Related Commands

".

Configuration Example

Security Authentication

Scenario Figure 13-7	
	● DEVICE-B is configured to the NTP client/server mode and provides NTP services requiring security authentication for DEVICE-C. The authentication key is "abcd". ● DEVICE-A is used as the reference clock source of DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● DEVICE-B configures DEVICE-A as the reference clock source. ● DEVICE-C configures DEVICE-B as the reference clock source.
DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Verification	● DEVICE-B sends a time synchronization packet that carries authentication information to 192.168.1.1 in order to synchronize time with DEVICE-A. ● Run the **show clock** command on DEVICE-B to check whether the time synchronization is successful.

13.4.3 Configuring NTP Access Control

Configuration Effect

Access control for NTP services provides a minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- Currently, the system does not support control query (used to control NTP servers by using network management devices, such as setting the leap second indicator or monitoring its working status). Though rule matching is implemented in the preceding sequence, no request related to control query is supported.
- If no access control rule is configured, all accesses are allowed. If any access control rule is configured, only accesses allowed by the rule can be implemented.

Related Configuration

Configuring the Access Control Rights for NTP

- Optional.
- Run the **ntp access-group** command to configure the access control rights and a corresponding ACL for NTP.

Verification

Run the **show run** command to verify the NTP configuration.

Related Commands

Configuring the Access Control Rights for NTP Services

Command	**ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*
Parameter Description	**peer**: allows time request and control query for local NTP services, and allows a local device to synchronize time with a remote system (full access rights). **serve**: allows time request and control query for local NTP services, but does not allow a local device to synchronize time with a remote system. **serve-only**: allows only time request for local NTP services. **query-only**: allows only control query for local NTP services. *access-list-number*: indicates the number of an IP ACL, ranging from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, refer to the *Configuring ACL*. *access-list-name*: indicates the name of an IP ACL. For details about how to create an IP ACL, refer to the *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP service matches rules in the sequence from the minimum access restriction to the maximum access restriction and uses the first matched rule. The matching sequence is peer, serve, serve-only, and query-only.

Configuration Example

Configuring NTP Access Control Rights

Configuration Steps	Allow only the device with the IP address of 192.168.1.1 to send a time synchronization request to a local device.
	Ruijie(config)# access-list 1 permit 192.168.1.1 Ruijie(config)# ntp access-group serve-only 1

13.5 Monitoring

Displaying

Description	Command
show ntp status	Displays the current NTP information.

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
debug ntp	Enables debugging.
no debug ntp	Disables debugging.

14 Configuring SNTP

14.1 Overview

The Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP), which is used to synchronize the clocks of computers on the Internet. SNTP is applied in scenarios where it is unnecessary to use all NTP functions.

NTP uses a complex algorithm and has higher requirements for the system whereas SNTP uses a simpler algorithm and provides higher performance. Generally, SNTP precision can reach about 1s, which meets the basic requirements of most scenarios. Since SNTP packets are the same as NTP packets, the SNTP client implemented on a device is fully compatible with an NTP server.

Protocols and Standards

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

14.2 Applications

Application	Description
Synchronizing Time with an NTP Server	A device is used as a client to synchronize time with an NTP server.

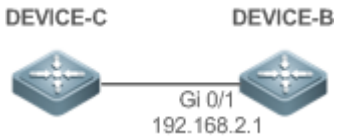
14.2.1 Synchronizing Time with an NTP Server

Scenario

As shown in Figure 14-1, DEVICE-B uses a local clock as the NTP clock reference source and provides time synchronization for DEVICE-C.

DEVICE-C is used as an SNTP client to synchronize time with DEVICE-B.

Figure 14-1



Deployment

- Specify DEVICE-B as the SNTP server of DEVICE-C.
- Enable SNTP for DEVICE-C.

14.3 Features

Basic Concepts

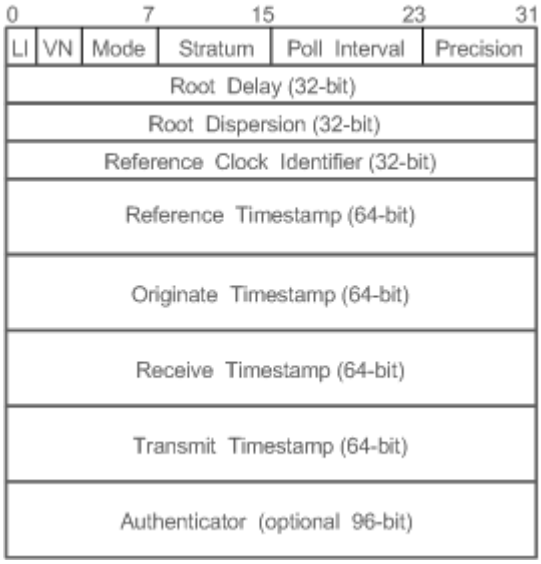
SNTP Packet

SNTPV4 is developed from NTP, which is intended to simplify the functions of NTP. It does not change the NTP specifications and the original implementation of NTP. The message format of SNTPV4 is the same as that of NTP defined in RFC1305, with only some data fields initialized into preset values.

As defined in RFC1305, SNTP uses User Datagram Protocol (UDP) packets for transmission and the used UDP port ID is 123.

Figure 14-2 shows the format of an SNTP time synchronization packet.

Figure 14-2 Format of an SNTP Time Synchronization Packet



- Leap Indicator(LI): indicates a 2-bit leap second indicator.

00: indicates no warning information; 01: indicates that there are 61 seconds in the previous minute; 10: indicates that there are 59 seconds in the previous minute; 11: indicates that the clock is not synchronized.

- Version Number(VN): indicates a 3-bit NTP/SNTP version number. The current version number is 3.
- Mode: indicates a 3-bit SNTP/NTP working mode.

0: indicates no definition; 1: indicates symmetric active; 2: indicates symmetric passive; 3: indicates a client; 4: indicates a server; 5: indicates broadcasting; 6: indicates control information; 7: reserved.

- Stratum: indicates the 8-bit stratum of a local clock. 0: indicates no definition; 1: indicates the master clock reference source; other values: indicate slave clock reference sources.
- Poll Interval: indicates the poll interval (seconds), which is a 8-bit integer.
- Precision: indicates the time precision (seconds) of a local clock, which is a 8-bit integer.

- Root Delay: indicates the round-trip time to the master clock reference source, which is a 32-bit integer.
- Root Dispersion: indicates the largest difference from the master reference clock source, which is a 32-bit integer.
- Reference Clock Identifier: indicates the 32-bit identifier of a reference clock source.
- Reference Timestamp: indicates a 64-bit timestamp, namely, the time that is set or corrected at the last time.
- Originate Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request leaves from a client.
- Receive Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization request packet arrives at a server.
- Transmit Timestamp: indicates a 64-bit timestamp, namely, the local time when a time synchronization response packet leaves from a server.
- Authenticator (optional): indicates authentication information.

Overview

Feature	Description
SNTP Time Synchronization	Synchronizes time from an SNTP/NTP server to a local device.

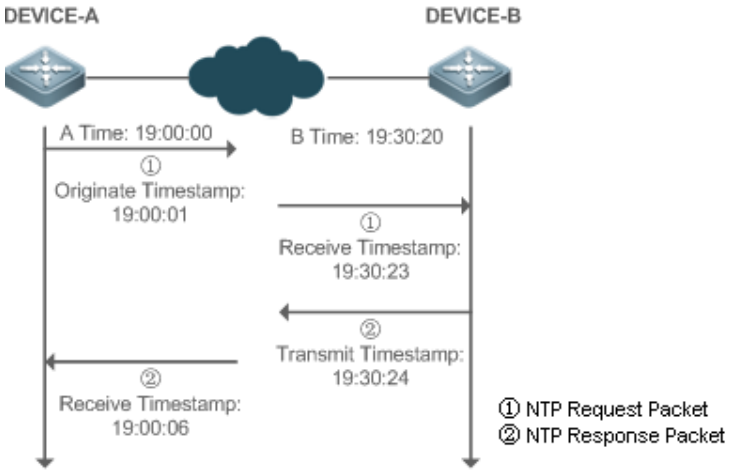
14.3.1 SNTP Time Synchronization

Working Principle

SNTP time synchronization is implemented by interaction of SNTP/NTP packets between a client and a server. The client sends a time synchronization packet to the server at intervals (half an hour by default). After receiving a response packet from the server, the client synchronizes time.

Figure 14-3 shows the format of an SNTP time synchronization packet.

Figure 14-3 Working Principle of SNTP



DEVICE-B (B for short) is used as an NTP reference clock source, DEVICE-A (A for short) is used as an SNTP client that synchronizes time with DEVICE-B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

- A sends an SNTP/NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in Originate Timestamp.
- After a 2-second network delay, the local time (T1) when B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
- B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in Transmit Timestamp.
- After a 2-second network delay, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

- A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.
- A obtains the packet round-trip delay of four seconds between A and B by using the formula (T3-T0)-(T2-T1).

Related Configuration

Enabling SNTP

- SNTP is disabled by default.
- Run the **sntp enable** command to enable SNTP.

Configuring an SNTP Server

- By default, no SNTP server is configured.
- Run the s**ntp server** command to specify an SNTP server.

Configuring the SNTP Time Synchronization Interval

- By default, the SNTP time synchronization interval is 1,800s.
- Run the **sntp interval** command to specify the time synchronization interval.

14.4 Configuration

Configuration	Description and Command	
Configuring SNTP	(Mandatory) It is used to enable SNTP.	
	sntp enable	Enables SNTP.
	sntp server	Configures the IP address of an SNTP server.
	(Optional) It is used to configure the SNTP time synchronization interval.	

Configuration	Description and Command	
	sntp interval	Configures the SNTP time synchronization interval.

14.4.1 Configuring SNTP

Configuration Effect

An SNTP client accesses an NTP server at fixed intervals to correct the clock regularly.

Notes

All time obtained through SNTP communication is Greenwich Mean Time (GMT). To obtain precise local time, you need to set the local time zone for alignment with GMT.

Configuration Steps

Enabling SNTP

- (Mandatory) SNTP is disabled by default.

Configuring the IP address of an SNTP Server

- (Mandatory) No SNTP/NTP server is configured by default.

Configuring the SNTP Time Synchronization Interval

- Optional.
- By default, a device synchronizes time every half an hour.

Verification

Run the **show sntp** command to display SNTP-related parameters.

Related Commands

Enabling SNTP

Command	**sntp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	SNTP is disabled by default. Run the **no sntp enable** global configuration command to disable SNTP.

Configuring the IP address of an SNTP/NTP Server

Command	**sntp server** *ip- address*

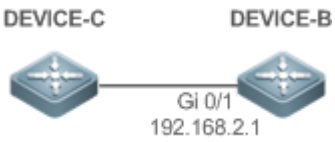
Parameter Description	*ip-address*: indicates the IP address of an NTP/SNTP server. No NTP/SNTP server is configured by default.
Command Mode	Global configuration mode
Usage Guide	Since SNTP is fully compatible with NTP, the server can be configured as a public NTP server on the Internet. Since SNTP packets are the same as NTP packets, the SNTP client is fully compatible with the NTP server. There are many NTP servers on the Internet. You can select an NTP server with a shorter delay as the SNTP server on your device.

Configuring the SNTP Time Synchronization Interval

Command	**sntp interval** *seconds*
Parameter Description	*seconds*: Indicates the time synchronization interval, ranging from 60s to 65,535s. The default value is 1,800s.
Command Mode	Global configuration mode
Usage Guide	Run this command to set the interval for an SNTP client to synchronize time with an NTP/SNTP server. ⚠ The interval configured here does not take effect immediately. To make it take effect immediately, run the **sntp enable** command.

Configuration Example

SNTP Time Synchronization

Scenario Figure 14-4	
	● DEVICE-B indicates an NTP server on the Internet. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	Enable SNTP for DEVICE-C and configure DEVICE-B as an NTP server.
DEVICE-C	`C#configure terminal` `C(config)# sntp server 192.168.2.1` `C(config)# sntp enable` `C(config)# exit`
Verification	● Run the **show clock** command on DEVICE-C to check whether the time synchronization is successful. ● Run the **show sntp** command on DEVICE-C to display the SNTP status and check whether the server is successfully configured.

14.5 Monitoring

Displaying

Description	Command
show sntp	Displays SNTP-related parameters.

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
debug sntp	Enables debugging.

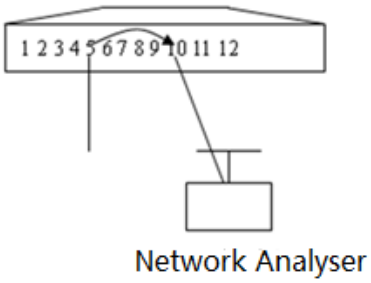
15 Configuring SPAN-RSPAN

15.1 Overview

The Switched Port Analyzer (SPAN) is to copy packets of a specified port to another switch port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

All input and output packets of a source port can be monitored through SPAN. For example, as shown in the following figure, all packets on Port 5 are mapped to Port 10, and the network analyzer connected to Port 10 receives all packets that pass through Port 5.

Figure 15-1 SPAN Configuration Instance



The SPAN function is mainly applied in network monitoring and troubleshooting scenarios, to monitor network information and rectify network faults.

15.2 Features

Basic Concepts

SPAN Session

A SPAN session is data streams between the SPAN source port and the destination port, which can be used to monitor the packets of one or more ports in the input, output, or both directions. Switched ports, routed ports, and aggregate ports (APs) can be configured as source ports or destination ports of SPAN sessions. Normal operations on a switch are not affected after ports of the switch are added to a SPAN session.

Users can configure a SPAN session on a disabled port but the SPAN session is inactive. A SPAN session is in the active state only after the port on which the SPAN session is configured is enabled. In addition, a SPAN session does not take effect after a switch is powered on. It is active only after the destination port is in the operational state. Users can run the **show monitor** [**session** *session-num*] command to display the operation status of a SPAN session.

SPAN Data Streams

A SPAN session covers data streams in three directions:

- Input data streams: All packets received by a source port are copied to the destination port. Users can monitor input packets of one or more source ports in a SPAN session. Some input packets of a source port may be discarded for some reasons (for example, for the sake of port security). It does not affect the SPAN function and such packets are still mirrored to the destination port.
- Output data streams: All packets transmitted by a source port are copied to the destination port. Users can monitor output packets of one or more source ports in a SPAN session. Packets transmitted from other ports to a source port may be discarded for some reasons and such packets will not be transmitted to the destination port. The format of output packets of a source port may be changed for some reasons. For example, after routing, packets transmitted from the source port are changed in source MAC addresses, destination MAC addresses, VLAN IDs, and TTLs, and their formats are also changed after copied to the destination port.
- Bidirectional data streams: Bidirectional data streams include input data streams and output data streams. In a SPAN session, users can monitor data streams of one or more source ports in the input and output directions.

Source Port

A source port is called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting. In a single SPAN session, users can monitor the input, output, and bidirectional data streams, and the number of source ports is not restricted.

A source port has the following features:

- A source port can be a switched port or a routed port.
- A source port cannot be used as a destination port simultaneously.
- A source port and a destination port can belong to the same VLAN or different VLANs.

Destination Port

A SPAN session has one destination port (called a monitoring port) for receiving packets copied from a source port.

A destination port has the following features:

- A destination port can be a switched port, routed port, or AP.
- A destination port cannot be used as a source port simultaneously.

Overview

Feature	Description
SPAN	Configures mirroring of ports on the same device.

15.2.1 SPAN

SPAN is used to monitor data streams on switches. It copies frames on one port to another switch port that is connected to a network analyzer or RMON analyzer so as to analyze the communication of the port.

Working Principle

When a port transmits or receive packets, SPAN, after checking that the port is configured as a SPAN source port, copies the packets transmitted and received by the port to the destination port.

Configuring a SPAN Source Port

Users need to specify a SPAN session ID and source port ID to configure a SPAN source port, and set the optional SPAN direction item to determine the direction of SPAN data streams or specify an ACL policy to mirror specific data streams.

Configuring a SPAN Destination Port

Users need to specify a SPAN session ID and destination port ID to configure a SPAN destination port, and set the optional switching function item to determine whether to enable the switching function and tag removal function on the SPAN destination port.

Related Configuration

The SPAN function is disabled by default. It is enabled only after a session is created, and the SPAN source and destination ports are configured. A SPAN session can be created when a SPAN source port or destination port is configured.

Configuring a SPAN Source Port

A SPAN session does not have a SPAN source port by default. Users can run the following command to configure a SPAN source port:

monitor session *session-num* **source interface** *interface-id* [**both** | **rx** | **tx**]

In the preceding command:

session-num: Indicates the SPAN session ID. The number of supported SPAN sessions varies with products.

interface-id: Indicates the SPAN source port to be configured.

rx: Indicates that only packets received by the source port are monitored after **rx** is configured.

tx: Indicates that only packets transmitted by the source port are monitored after **tx** is configured.

both: Indicates that packets transmitted and received by the source port are copied to the destination port for monitoring after **both** is configured, that is, **both** includes **rx** and **tx**. If none of **rx**, **tx**, and **both** is selected, **both** is enabled by default.

Configuring a SPAN Destination Port

A SPAN session does not have a SPAN destination port by default. Users can run the following command to configure a SPAN destination port:

monitor session *session-num* **destination interface** *interface-id* [**encapsulation replicate** | **switch**]

In the preceding command:

encapsulation replicate: Forcibly removes tags (VLAN information carried in packets) from packets if this option is enabled.

switch: Indicates that the SPAN destination port only receives packets mirrored from the SPAN source port and discards other packets if this option is disabled, and receives both packets mirrored from the SPAN source port and packets from

non-source ports if this option is enabled, that is, the communication between this destination port and other devices is not affected.

When the SPAN destination port is configured, the relevant function is disabled by default if **encapsulation replicate** or **switch** is not configured.

15.3 Configuration

Configuration	Description and Command	
Configuring SPAN Basic Functions	(Mandatory) It is used to create SPAN.	
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Configures a SPAN source port.
	monitor session *session-num* **destination interface** *interface-id*[**switch | encapsulation replicate**]	Configures a SPAN destination port.

15.3.1 Configuring SPAN Basic Functions

Configuration Effect

- Configure a source and destination ports for a SPAN session.
- Configure a destination port to monitor any packets transmitted and received by a source port.

Notes

- If a source port or destination port is added to an AP, the source port or destination port exits from a SPAN session.
- If the switch function is disabled on a SPAN destination port, the destination port receives only mirrored packets and discards other packets that pass through the port. After the switch function is enabled, the destination port can receive non-mirrored packets.

Configuration Steps

Configuring a SPAN Session

- Global configuration mode. Mandatory.
- You can configure a SPAN session when configuring a SPAN source port or destination port, or when configuring a specified VLAN or some VLANs as a data source or data sources of SPAN.

Configuring a SPAN Source Port

- Global configuration mode. Mandatory.
- You can select the SPAN direction when configuring a SPAN source port. The **both** direction is configured by default, that is, both transmitted and received packets are monitored.

Configuring a SPAN Destination Port

Global configuration mode. Mandatory.

A SPAN session is active only when a SPAN source port is configured (or a VLAN is specified as the data source of SPAN) and a SPAN destination port is configured.

Verification

- Run the **show monitor** command or the **show running** command to verify the SPAN configuration. Alternatively, conduct packet capture analysis on the SPAN destination port and check whether the SPAN function takes effect according to the captured packets.

Related Commands

Configuring a SPAN Source Port

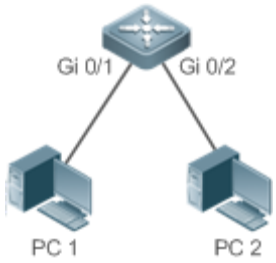
Command	**monitor session** *session-num* **source interface** *interface-id* [**both** | **rx** |**tx**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. **both:** Indicates that packets in the input and output directions are monitored. It is the default value. **rx:** Indicates that packets in the input direction are monitored. **tx:** Indicates that packets in the output direction are monitored.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a SPAN Destination Port

Command	**monitor session** *session-num* **destination interface** *interface-id*[**switch** | **encapsulation replicate**]
Parameter Description	*session-num:* Indicates the ID of a SPAN session. *interface-id*: Indicates the interface ID. **switch:** Indicates that the switching function is enabled on the SPAN destination port. It is disabled by default. **encapsulation replicate:** Indicates that the encapsulation function is enabled on the mirroring port. Mirrored packets are untagged forcibly if this function is enabled. It is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

The following uses SPAN as an example.

Scenario **Figure 15-2**	
Configuration Steps	● As shown in Figure 1-5, add ports Gi 0/1 and Gi 0/2 of Device A to VLAN 1. ● Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24. ● Set IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24 respectively. ● Configure SPAN for Device A and configure ports Gi 0/1 and Gi 0/2 as the source port and destination port of SPAN respectively.
A	`Ruijie# configure` `Ruijie(config)# vlan 1` `Ruijie(config-vlan)# exit` `Ruijie(config)# interface vlan 1` `Ruijie(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0` `Ruijie(config-if-VLAN 1)# exit` `Ruijie(config)# monitor session 1 source interface gigabitEthernet 0/1` `Ruijie(config)# monitor session 1 destination interface gigabitEthernet 0/2`
Verification	Run the **show monitor** command to check whether SPAN is configured correctly. After successful configuration, PC 1 sends ping packets to SVI 1 and PC 2 conducts monitoring by using the packet capture tool.
A	`Ruijie# show monitor` `sess-num: 1` `span-type: LOCAL_SPAN` `src-intf:` `GigabitEthernet 0/1 frame-type Both` `dest-intf:` `GigabitEthernet 0/2`

Common Errors

- The session ID specified during configuration of the SPAN source port is inconsistent with that specified during configuration of the SPAN destination port.

- Packet loss may occur if packets of a port with large bandwidth are mirrored to a port with small bandwidth.

15.4 Monitoring

Displaying

Description	Command
Displays all mirroring sessions existing in the system.	**show monitor**
Displays a specified mirroring session.	**show monitor session** *session-id*

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs SPAN.	**debug span**

16 Configuring Time Range

16.1 Overview

Time Range is a time-based control service that provides some applications with time control. For example, you can configure a time range and associate it with an access control list (ACL) so that the ACL takes effect within certain time periods of a week.

16.2 Typical Application

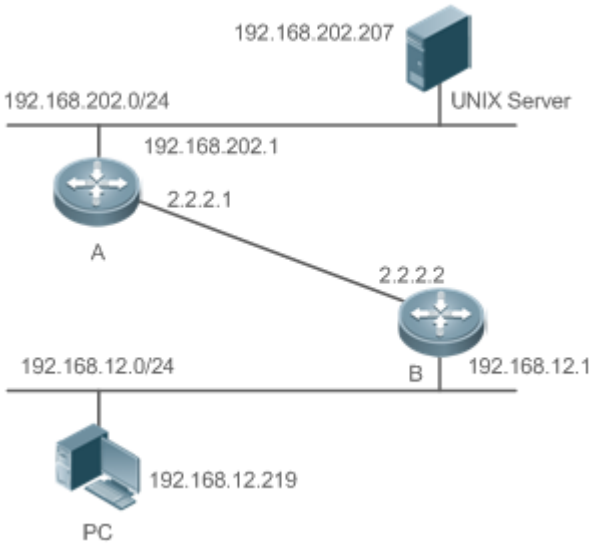
Typical Application	Scenario
Applying Time Range to an ACL	Apply a time range to an ACL module so that the time-based ACL takes effect

16.2.1 Applying Time Range to an ACL

Application Scenario

An organization allows users to access the Telnet service on a remote Unix host during working hours only, as shown in Read-write: Provide the read/write permission of all MIB variables for authorized management workstations.

Figure 16-1



Note	Configure an ACL on device B to implement the following security function: Hosts in network segment 192.168.12.0/24 can access the Telnet service on a remote Unix host during normal

	working hours only.

Functional Deployment

- On device B, apply an ACL to control Telnet service access of users in network segment 192.168.12.0/24. Associate the ACL with a time range, so that the users' access to the Unix host is allowed only during working hours.

16.3 Function Details

Basic Concepts

↘ Absolute Time Range

The absolute time range is a time period between a start time and an end time. For example, [12:00 January 1 2000, 12:00 January 1 2001] is a typical absolute time range. When an application based on a time range is associated with the time range, a certain function can be effective within this time range.

↘ Periodic Time

Periodic time refers to a periodical interval in the time range. For example, “from 8:00 every Monday to 17:00 every Friday” is a typical periodic time interval. When a time-based application is associated with the time range, a certain function can be effective periodically from every Monday to Friday.

Features

Feature	Function
Using Absolute Time Range	Sets an absolute time range for a time-based application, so that a certain function takes effect within the absolute time range.
Using Periodic Time	Sets periodic time or a time-based application, so that a certain function takes effect within the periodic time.

16.3.1 Using Absolute Time Range

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the absolute time range. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

↘ Configuring Time Range

No time range is configured by default.

Use the **time-range** *time-range-name* command to configure a time range.

↘ Configuring Absolute Time Range

The absolute time range is [00:00 January 1, 0, 23:59 December 31, 9999] by default.

Use the **absolute** { [**star**t *time date*] | [**end** *time date*] } command to configure the absolute time range.

16.3.2 Using Periodic Time

Working Principle

When a time-based application enables a certain function, it determines whether current time is within the period time. If yes, the function is effective or ineffective at the current time depending on specific configuration.

Related Configuration

↘ Configuring Time Range

No time range is configured by default.

Use the **time-range** *time-range-name* command to configure a time range.

↘ Configure Periodic Time

No periodic time is configured by default.

Use the **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time* command to configure periodic time.

16.4 Configuration Details

Configuration Item	Suggestions and Related Commands	
Configuring Time Range	⚠ Mandatory configuration. Time range configuration is required so as to use the time range function.	
	time-range *time-range-name*	Configures a time range.
	⚠ Optional configuration. You can configure various parameters as necessary.	
	absolute { [**star**t *time date*] | [**end** *time date*] }	Configures an absolute time range.
	periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*	Configures periodic time.

16.4.1 Configuring Time Range

Configuration Effect

- Configure a time range, which may be an absolute time range or a periodic time interval, so that a time-range-based application can enable a certain function within the time range.

Configuration Method

↘ Configuring Time Range

- Mandatory configuration.
- Perform the configuration on a device to which a time range applies.

Configuring Absolute Time Range

- Optional configuration.

Configuring Periodic Time

- Optional configuration.

Verification

- Use the **show time-range** [*time-range-name*] command to check time range configuration information.

Related Commands

Configuring Time Range

Command Syntax	**time-range** *time-range-name*
Parameter Description	*time-range-name*: name of the time range to be created.
Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range, then you can configure relevant time control in time range configuration mode.

Configuring Absolute Time Range

Command Syntax	**absolute** { [**start** *time date*] | [**end** *time date*] }
Parameter Description	**start** *time date*: start time of the range. **end** *time date*: end time of the range.
Command Mode	Time range configuration mode
Usage Guide	Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.

Configuring Periodic Time

Command Syntax	**periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*
Parameter Description	*day-of-the-week*: the week day when the periodic time starts or ends *time*: the exact time when the periodic time starts or ends
Command	Time range configuration mode

Mode	
Usage Guide	Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.

16.5 Monitoring and Maintaining Time Range

Displaying the Running Status

Function	Command
Displays time range configuration.	**show time-range** [*time-range-name*]

Specifications and Limitations

This section lists the specifications and limitations of features supported on wireless controller products.

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>WLAN AP Management</td><td>
1. WS6024 V1.0 products do not support expanded license. The maximum number of other APs has a lower limit of 1 and a variable upper limit according to different license. Here are accessible ranges and defaults of various products:
<table>
<tr><th>Model</th><th>Accessible Range</th><th>Default Value</th></tr>
<tr><td>WS6008</td><td>1-224</td><td>32</td></tr>
<tr><td>WS6108</td><td>1-320</td><td>32</td></tr>
<tr><td>WS6816</td><td>1-3200</td><td>128</td></tr>
<tr><td>M18000-WS-ED</td><td>1-2560</td><td>128</td></tr>
<tr><td>M8600E-WS-ED</td><td>1-2560</td><td>128</td></tr>
<tr><td>WS6024</td><td>1-24</td><td>24</td></tr>
</table>
2. The range of WLAN ID varies with product model.
WS6008 V1.0 and WS6108 V1.0: 1-2048;
WS6024 V1.0, WS6816V1.0 and N18000-WS-ED/M86E-WS-ED: 1-4094.
3. Virtualized AP is not supported on WS6024.
4. Virtualized AP is supported on the following AP products: AP520-I, AP520-I(G2), AP520(W2), AP720-I, AP720-L, AP740-I and AP740-I(C).
5. The offline-ssid command is supported on the following AP products: AP130(W2), AP520-I, AP520-I(G2), AP520(W2), AP720-I, AP720-L, AP740-I and AP740-I(C).
</td></tr>
<tr><td>WLAN CAPWAP</td><td>
1. The wired-vlan command is supported only on the AP130(W2) AP products.
2. The wired-interface command is supported only on the AP130(W2) AP devices.
</td></tr>
<tr><td>WALN STA Management</td><td>
The maximum number of wireless STAs has a lower limit of 1 and a variable upper limit on different models. Here are accessible ranges and defaults of various products:

In AC configuration mode:
<table>
<tr><th>Model</th><th>Accessible Range</th><th>Default Value</th></tr>
<tr><td>WS6008</td><td>1-7168</td><td>7168</td></tr>
</table>

</td></tr>
</table>

	WS6108	1-10240	10240
	WS6816	1-81920	81920
	M18000-WS-ED	1-81920	81920
	M8600E-WS-ED	1-81920	81920
	WS6024	1-768	768

- In WLAN configuration mode, the range is same as that in AC configuration mode; no defaults;
- In AP group configuration mode/AP configuration mode(for offline AP), range: 1-1,536; no defaults;
- In AP configuration mode:

Model	Upper Limit	Default Value
AP130(W2) V1.0	32	32
AP740-I V1.x	612	80
AP740-I(C) V1.x	512	64

WLAN Hot Backup

1. Hot backup is not supported on WS6024.
2. Only WS6816, M18000-WS-ED and M8600E-WS-ED can be configured as master wireless controllers.

WLAN WBS

1. Management frame power configuration is not supported on AP740-I.
2. The mask of transmitting or receiving antenna on AP740-I and AP740-I(C) cannot be configured as 2.
3.

WLAN CPU Protection

CPU protection is not supported on WS6024.

The following table lists the default bandwidth limits for the wireless controller products.

Model	Defaults (pps)
M6000-WS	40
WS6008	40
WS6108	40
WS6816	600
M18000-WS-ED	600

M8600E-WS-ED	600

The following table lists the default bandwidth limits for the specified type of packets on the wireless controller products.

Model Packet Type	WS6008	WS6108
arp	1000	1000
bpdu	128	128
capwap-disc	128	128
d1x	480	480
dhcp-option82	128	128
dhcp-relay-client	128	128
dhcp-relay-server	128	128
dhcps	128	128
igmp	500	500
ipmc	128	128
ipv6-nans	128	128
isis	128	128
lldp	128	128
ospf	600	600
ospfv3	600	600
pppoe	128	128
pim	1000	1000
rip	128	128
ripng	600	600
tcp80	1200	1200
tcp443	100	100
vrrp	128	128

The following table lists the default bandwidth limits for the specified type of packets on the AP products.

Packet Type	Defaults (pps)
arp	100
bpdu	128
capwap-disc	128
d1x	128
dhcp-option82	128

	dhcp-relay-client: 128 dhcp-relay-server: 128 dhcps: 128 igmp: 200 ipmc: 128 ipv6-nans: 128 isis: 128 lldp: 128 ospf: 600 ospfv3: 600 pppoe: 1,000 pim: 128 rip: 128 ripng: 600 tcp80: 1,200 tcp443: 100 vrrp: 128
WLAN Ethernet Management	1. The **wired-rate** *value* **port** *port-id* command is supported on MAP552, MAP552-W and MAP552(S). **Model** / **Maximum Speed** MAP552: 100 Mbps MAP552-W: 100 Mbps MAP552(S): 100 Mbps
WLAN Forwarding	1. Centralized forwarding mode is not supported on WS6024. 2. AC forwarding mode is only supported on WS6008 and WS6108.
NFPP	NFPP is not supported on WS6024. The following table lists the default ARP guard rate limits and attack thresholds for the wireless controller products.

Model	Default ARP Guard Rate Limit (pps)			Default ARP Attack Threshold (pps)		
	per-src-ip	src-mac	per-port	per-src-ip	per-src-mac	per-port
WS6008	30	30	480	60	60	960
WS6108	30	30	480	60	60	960
WS6816	30	30	1920	60	60	3840

M18000-WS-ED	30	30	1920	60	60	3840
M8600E-WS-ED	30	30	1920	60	60	3840

The following table lists the default ICMP guard rate limits and attack thresholds for the wireless controller products.

Model	Default ICMP Guard Rate Limit (pps)		Default ICMP Attack Threshold (pps)	
	per-src-ip	per-port	per-src-ip	per-port
WS6008	400	500	600	800
WS6108	400	500	600	800
WS6816	800	1,000	1,200	1,500
M18000-WS-ED	800	1,000	1,200	1,500
M8600E-WS-ED	800	1,000	1,200	1,500

The following table lists the default DHCP guard rate limits and attack thresholds for the wireless controller products.

Model	Default DHCP Guard Rate Limit (pps)		Default DHCP Attack Threshold (pps)	
	per-src-mac	per-port	per-src-mac	per-port
WS6008	5	300	10	512
WS6108	5	300	10	512
WS6816	5	1,200	10	1,500
M18000-WS-ED	5	1,200	10	1,500
M8600E-WS-ED	5	1,200	10	1,500

The following table lists the default DHCPv6 guard rate limits and attack thresholds for the wireless controller products.

Model	Default DHCPv6 Guard Rate Limit (pps)		Default DHCPv6 Attack Threshold (pps)	
	per-src-mac	per-port	per-src-mac	per-port
WS6008	5	300	10	512
WS6108	5	300	10	512
WS6816	5	1,200	10	1,500
M18000-WS-ED	5	1,200	10	1,500
M8600E-WS-ED	5	1,200	10	1,500

The following table lists the default ND guard rate limits and attack thresholds for the wireless controller

products.

Model	Default ND Guard Rate Limit (pps)			Default ND Attack Threshold (pps)		
	ns-na	rs	ra-redirect	ns-na	rs	ra-redirect
WS6008	100	50	50	200	100	100
WS6108	100	50	50	200	100	100
WS6816	2,000	500	500	4,000	800	800
M18000-WS-ED	2,000	500	500	4,000	800	800
M8600E-WS-ED	2,000	500	500	4,000	800	800

The following table lists the default bandwidth of each type of packets for centralized rate limiting and distribution on the wireless controller products.

Model	MANAGE	ROUTE	PROTOCOL
WS6008	3,500	3,000	3,000
WS6108	3,500	3,000	3,000
WS6816	8,192	10,000	8,192
M18000-WS-ED	8,192	10,000	8,192
M8600E-WS-ED	8,192	10,000	8,192

Management Port	MGMT ports are supported on the following products: WS6816 and M18000-WS-ED.
Security	1. PPSK is supported on the following products: WS6024, WS6008 and WS6108. 2. Bonjour Gateway is not supported on WS6024. 3. 802.11R is not supported on AP720-L.
VAC	VAC is not supported on WS6024 or M6000-WS.
RIPng	RIPng is supported on the following products: WS6816 and M18000-WS-ED.
OSPF	OSPFv3 is supported on the following products: WS6816 and M18000-WS-ED.
WAPI	For AP740-I, AP740-I(C), AP720-I, AP520(W2) and AP130(W2), the WAPI function is for test only and not official released.
Smart Antenna	Smart antenna is supported on the following products: AP520-I(G2), AP740-I and AP720-I.
FSS	The FSS function is supported on the following products: AP520-I(G2), AP520(W2) and AP130(W2).

	The FSS function on the AP740-I, AP740-I(C) and AP720-I is only for test and not official released.
RLDP	The RLDP function is only supported on WS6024.
DLDP	The DLDP function is only supported on WS6024.
LLDP	The LLDP function is only supported on WS6024.