



Ruijie RG-S2915-L Series Switches

S2915-L_RGOS 11.4(1)B82

Web-based Configuration Guide

Document Version: V1.0
Date: November 16th, 2022
Copyright © 2022 Ruijie Networks

Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark  and  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: <https://www.ruijienetworks.com/rita>

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in bold font.
<i>Italic font</i>	Arguments for which you supply values are in <i>italic</i> font.
[]	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.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

 **Warning**

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

 **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

 **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

 **Specification**

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 Configuring Switch Eweb

1.1 Overview

You can access the web management system (that is, Eweb) of switches through a browser, such as Internet Explorer (IE), to manage the switches.

Web management involves the web server and web client. The web server, integrated into a switch, is used to receive and process requests from a client (reading web files or executing commands), and return processing results to the client. The web client is usually a web browser, such as IE.

✔ Specification

This document applies only to S2915-L series switches.

1.2 Application

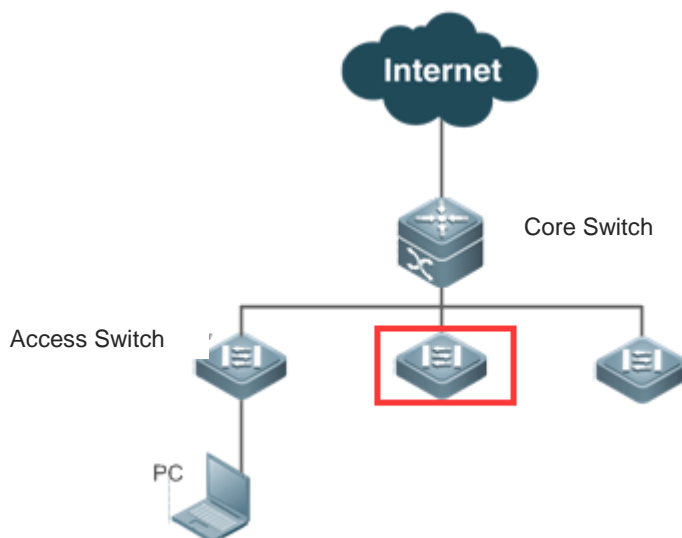
Application	Description
Managing Switches through the Eweb	After switches are configured, you can access the Eweb through a browser.

1.2.1 Managing Switches through the Eweb

1. Scenario

As shown in Figure 1-1, you can access the Eweb of an access switch or aggregation switch through a browser to manage and configure the switch.

Figure 1-1



Note

The device enclosed in the red rectangle in Figure 1-1 is the access switch. Ensure that the switch can be pinged successfully from the PC. Then you can access the Eweb of the switch.

2. Deployment

(1) Configuration Environment Requirements

Client requirements:

- You can manage the switch by logging in to the web management interface of the switch through the browser of the web management client. Clients refer to PCs or other mobile terminals such as laptops.
- Browser: IE8–IE11, Google Chrome, and 360 Browsers are supported. Exceptions such as garble or format errors may occur if an unsupported browser is used.
- Resolution: The recommended resolution is 1024*768, 1280*1024, 1440*960, or 1920*1080. If other resolutions are used, exceptions such as format errors or misalignment occur.

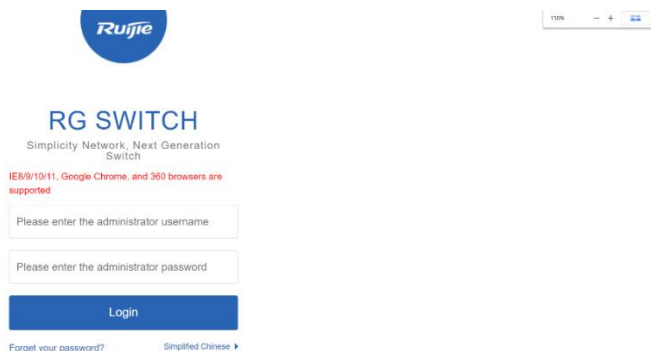
Note

Eweb configuration and command line interface (CLI) configuration can be performed simultaneously. After CLI configuration is complete, enter the **write** command to save the configuration. If you open the web page, refresh the page to ensure that Eweb and CLI configurations are synchronized.

(2) Logging In to the Web Management Platform

Enter `http://X.X.X.X` (management IP address) in the browser and press Enter to access the **Login** page, as shown in Figure 1-2.

Figure 1-2 Login Page



Enter the username and password and click **Login**. The following table provides the default username and password.

Table 1-1

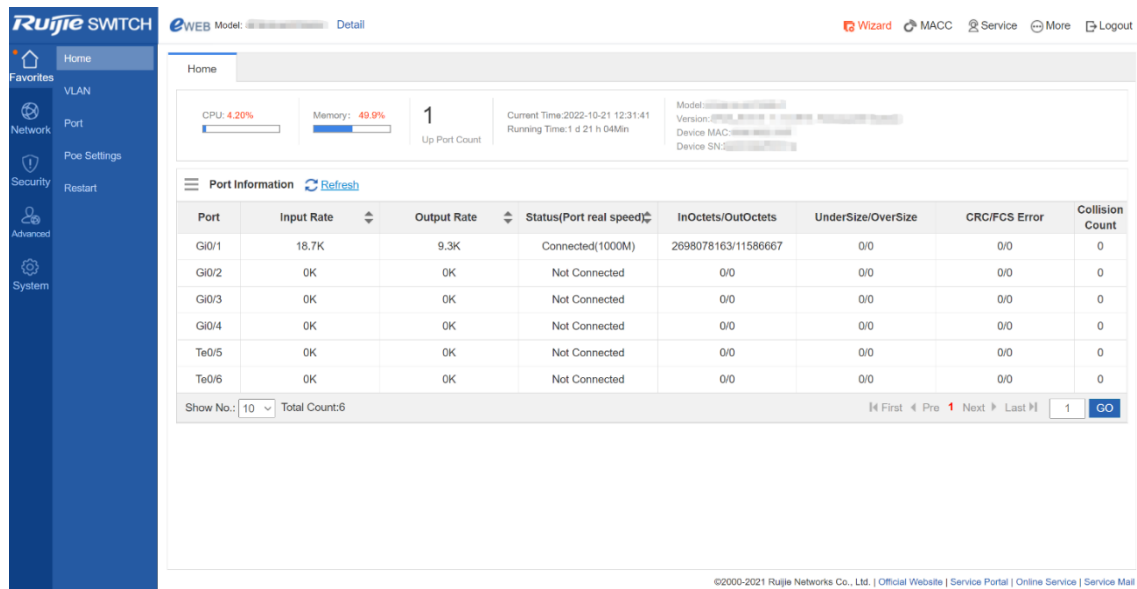
Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions

Note

When you log in by using the default username and password, the system requests you to change the password to ensure security.

After authentication is successful or the password is changed, the Eweb homepage is displayed, as shown in Figure 1-3.

Figure 1-3 Eweb Homepage



Note

For details about Eweb pages, see [Eweb Management System](#).

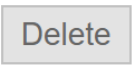










1.3 Eweb Management System

Basic Concepts

Icons and Buttons on the GUI

Table 1-2

Icon/Button	Description
	Edit the selected record.

	Delete the selected record.
	Enable or disable the function.
	Available port. After you click or select the icon, the port becomes selected.
	Unavailable port.
	Selected port.
	Aggregated port. The digit in the port indicates the number of the aggregated port.
	Trunk port. It is displayed on the panel of the VLAN Management/VLAN Settings page.
	Submit and save input information.
	Add settings.
	Delete settings.
All Invert Deselec	Batch configuration of panel ports, which is on the right bottom corner of the panel. Note: Note: You can use this function only when you can select multiple ports on the panel.
	An input box marked with this symbol indicates that the item is mandatory.

Features

The following table describes feature configurations of secondary menu items in the left navigation tree of the web GUI.

Table 1-3

Feature	Description
Home	Displays port information and overall device information.
VLAN Management	Sets VLANs and trunk ports.
Port Management	Configures basic information about ports, aggregated ports, port mirroring, and port rate limit.
POE Settings	Configures PoE in the system and on ports.

Restart	Restart the switch.
MAC Address	Sets static addresses and filter addresses.
Routing	Sets routes.
STP	Configures basic information of global STP, STP ports, and RSTP.
IGMP Settings	Sets Internet Group Management Protocol (IGMP) snooping.
DHCP Snooping	Sets DHCP snooping.
Gateway Anti-ARP-Snooping	Configures anti-ARP-spoofing on the gateway, Address Resolution Protocol (ARP) check, dynamic ARP inspection (DAI), and ARP entries.
IP Source Guard	Configures ports and user binding.
NFPP	Displays information related to Network Foundation Protection Policy (NFPP).
Storm Control	Control storms.
Port Protection	Configures port protection.
ACL	Configures access control lists (ACLs), set the ACL time, and applies ACLs.
Settings	Sets the system time, changes the password, restores to factory settings, and configures the enhancement function, SNMP and DNS.
Upgrade	Performs local upgrade and online upgrade of web packages.
System Logging	Sets the log server and queries system logs.
CWMP	Configures CPE WAN Management Protocol (CWMP).
Detection	Configures ping test, tracer test, cable detection, and one-click collection.
Web Console	Imitates the mechanism of CLI commands.

1.3.1 Initialization Configuration

Figure 1-4 Initialization Configuration

The screenshot shows a 'Wizard' window with the following configuration fields:

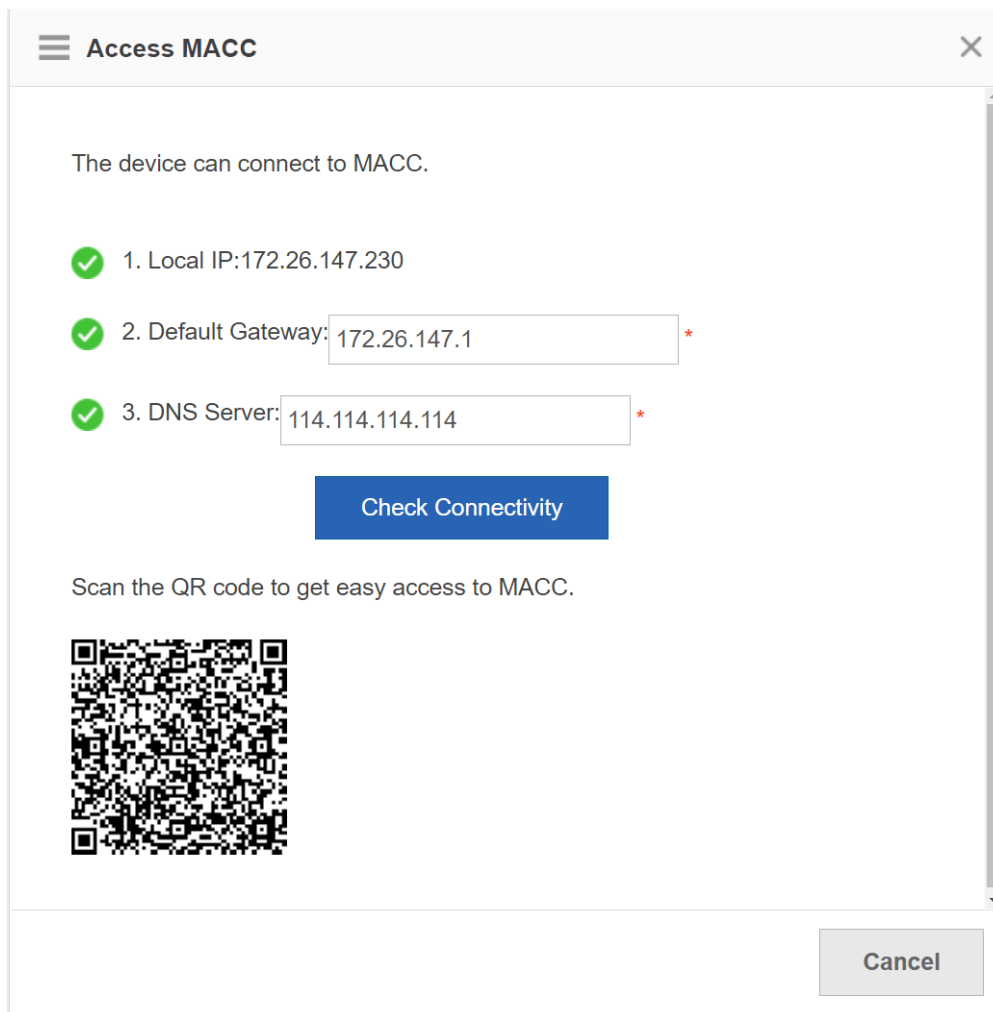
- Mgmt Port: Gi0/1
- IP: 172.26.147.230
- Mask: 255.255.255.0
- Gateway: 172.26.147.1
- DNS: 114.114.114.114
- IPv6/Mask: [] []
- IPv6 gateway: []
- Reset Time: 2022-10-21 12:35
- Time Zone: UTC+8(Beijing, CCT) [v]

Buttons: Save, Cancel

Configure the management VLAN ID, IP address, subnet mask, default gateway and DNS server. Click **Save** and the message "Configuration succeeded." is displayed.

1.3.2 MACC Management

Figure 1-5 MACC Management



After configuring the device IP, default gateway and DNS server, click **Check Connectivity** to check whether the device connects to MACC. Scan the QR code to add the device to MACC.

1.3.3 Common

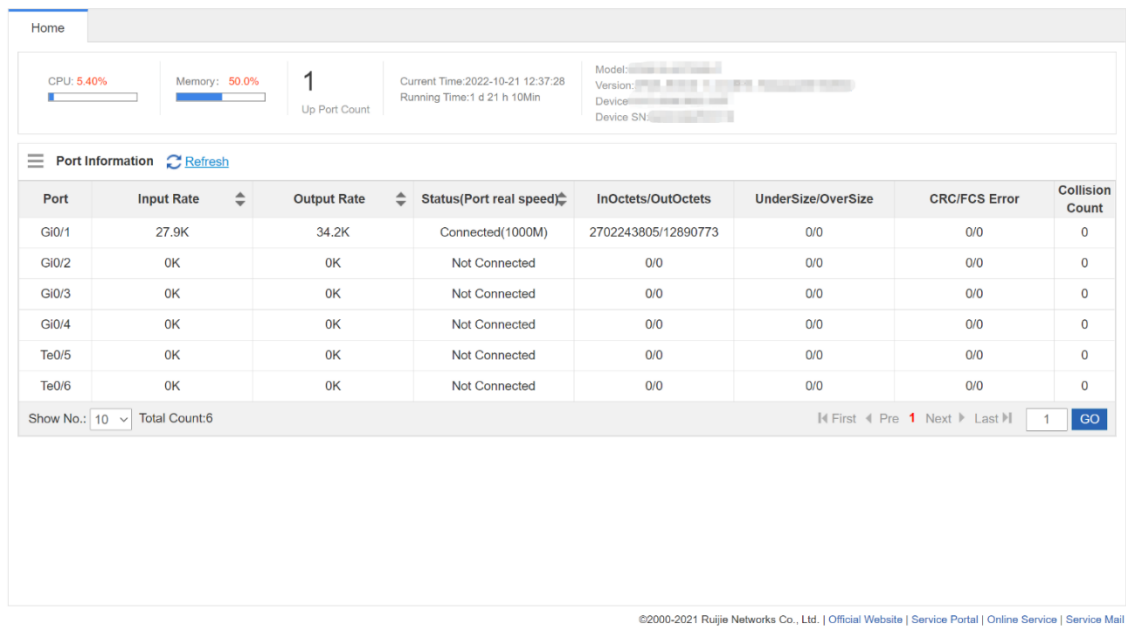
Click the primary menu **Common** to access the secondary menu, including **Home**, **VLAN Management**, **Port Management**, **PoE Settings** and **Restart**.

1. Home

The **Home** page displays device configurations, basic port information, and port statistics.

Figure 1-6 shows the **Home** page.

Figure 1-6 Home



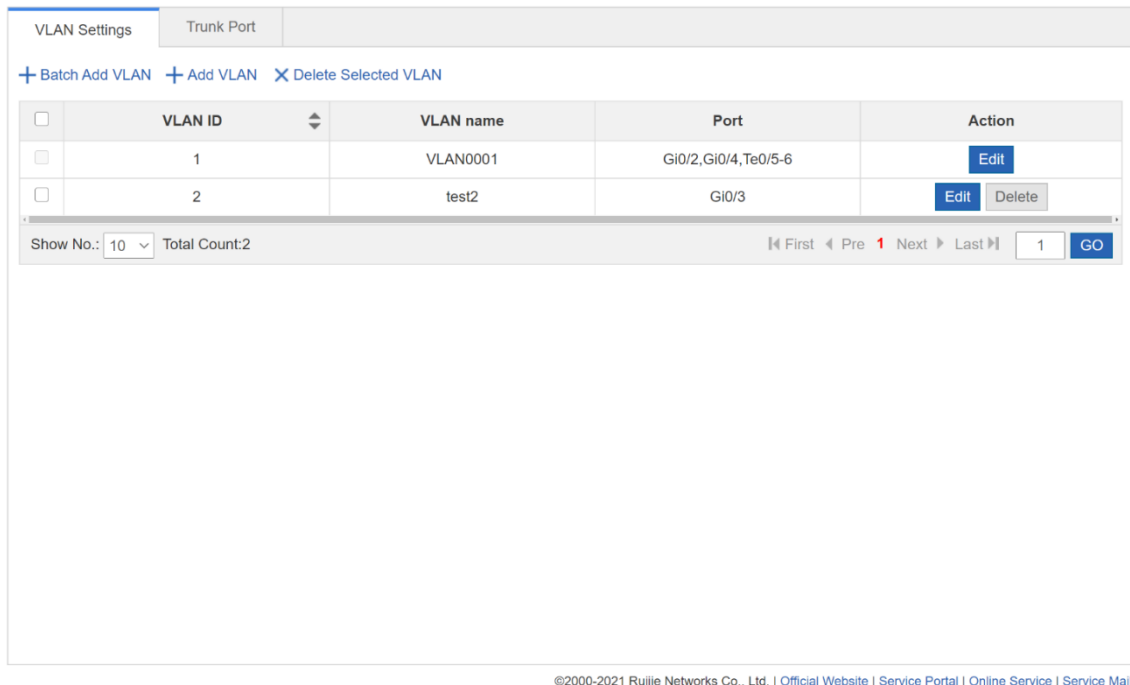
2. VLAN Management

The **VLAN Management** page consists of **VLAN Settings** and **Trunk Port**.

(1) VLAN Settings

Figure 1-7 shows the **VLAN Settings** page.

Figure 1-7 VLAN Settings



- Adding a VLAN

The VLAN ID is mandatory. Other parameters are optional. Click **Save** and the message “Configuration succeeded.” is displayed. The added VLAN is displayed in the list.

- Editing a VLAN

In the VLAN list, click **Edit** in the **Action** column for a VLAN. Information about the VLAN is displayed. Edit the information, click **Save**. The message “Edit succeeded” is displayed.

- Deleting a VLAN
 - Select multiple records in the VLAN list and click **Delete Selected VLAN** to delete the records in a batch.
 - in the VLAN list, click **Delete** in the **Action** column for a VLAN. The message “Are you sure you want to delete the VLAN ?” is displayed. Click **OK**. The message “Delete succeeded.” is displayed, indicating that the VLAN is deleted.

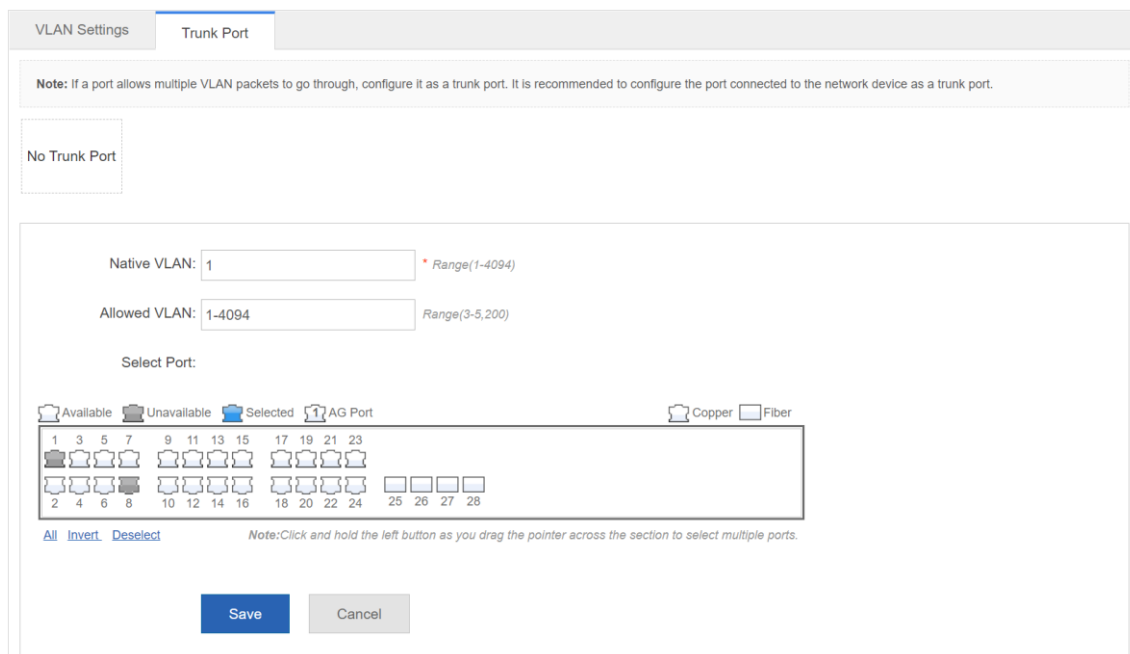
Note

VLAN 1 is the default VLAN. It can be only modified but cannot be deleted.

(2) Trunk Port

Figure 1-8 below shows the **Trunk Port** page.

Figure 1-8 Trunk Port



- Adding a Trunk Port

Select a port on the panel, enter the ranges of Native VLAN and Allowed VLAN (3-5,8,10 for example). Click **Save**. The message “Configuration succeeded” is displayed. The added trunk port is displayed in the trunk port list.

- Editing a Trunk Port

Select a trunk port in the trunk port list. Its information is displayed. Edit the information and click **Edit**. The message “Configuration succeeded” is displayed.

- Deleting a Trunk Port

Move the cursor to a trunk port in the trunk port list, click **Delete**. The message “Are you sure you want to delete the trunk port?” is displayed. Click **OK**. The message “Delete succeeded.” is displayed, indicating that the trunk port is deleted.

- Batch Deleting Trunk Ports

In the trunk port list, select trunk ports to be deleted and click **Batch Del**. The message “Are you sure you want to delete the trunk port?” is displayed. Click **OK**. The message “Delete succeeded.” is displayed, indicating that the trunk ports are deleted.

3. Port Management

The **Port** page allows you to configure basic settings about ports, aggregate port, and port mirroring.

(1) Port Settings

Figure 1-9 Port Settings

The screenshot shows the 'Port Settings' page with tabs for 'Port Settings', 'Aggregate port', and 'Port Mirroring'. It includes buttons for '+ Batch Add' and '+ Add SVI'. There are two expandable sections: 'L3 Port' and 'L2 Port'.

L3 Port Table:

Port	Up/Down	IP	Mask	IPv6	Description	Action
Gi0/1	Down					Edit Delete
Gi0/8	Up	10.110.69.99	255.255.255.0			Edit Delete
VLAN 1	Up					Edit Delete

Navigation: Show No.: 10 Total Count:3 | First | Pre 1 Next | Last | 1 GO

L2 Port Table:

Port	Up/Down	Port Type	Access VLAN	Native VLAN	Permit VLAN	Description	Action
Gi0/2	Down	ACCESS	1	1			Edit Detail
Gi0/3	Down	ACCESS	1	1			Edit Detail
Gi0/4	Down	ACCESS	1	1			Edit Detail
Gi0/5	Down	ACCESS	1	1			Edit Detail
Gi0/6	Down	ACCESS	1	1			Edit Detail
Gi0/7	Down	ACCESS	1	1			Edit Detail
Gi0/9	Down	ACCESS	1	1			Edit Detail
Gi0/10	Down	ACCESS	1	1			Edit Detail
Gi0/11	Down	ACCESS	1	1			Edit Detail
Gi0/12	Down	ACCESS	1	1			Edit Detail

Navigation: Show No.: 10 Total Count:30 | First | Pre 1 2 3 Next | Last | 1 GO

- Batch Configuring Ports

Select ports to be configured and select the port status, rate, and mode. **Keep** indicates that the system retains the original configuration. You can set **Keep** for some settings to batch configure only one or two settings.

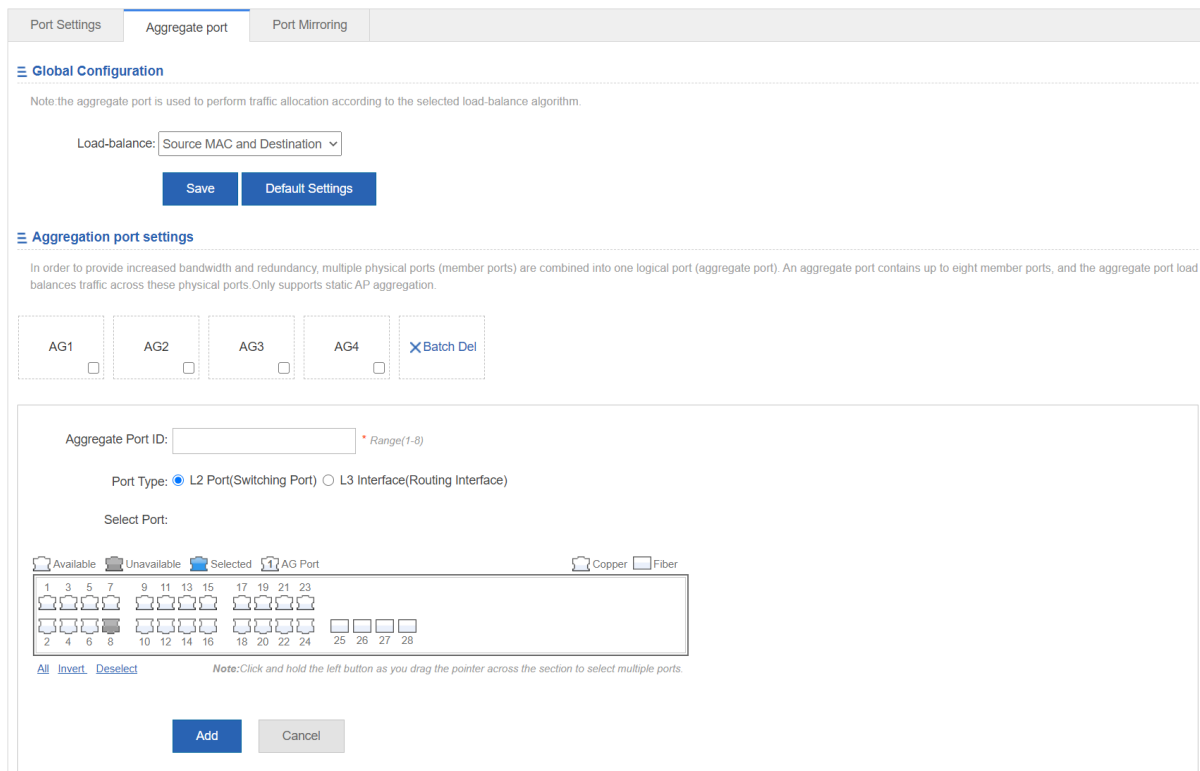
- Editing a Port

Click **Edit** in the **Action** column of the port list. The port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

(2) Port Aggregation

Figure 1-10 shows the **Aggregate Port** page.

Figure 1-10 Aggregate Port



- Adding an Aggregated Port

Enter an aggregated port ID, select member ports, and click **Add**. The message “Configuration succeeded.” indicating that the aggregated port is added. The port panel displays the successfully added aggregated port.

- Editing an Aggregated Port

Aggregated ports displayed on the panel cannot be selected. To edit an aggregated port, click the aggregated port in the aggregated port list. Its member ports become selected. Click a port to cancel selection and then click **Edit** to modify the aggregated port.

- Deleting an Aggregated Port

In the aggregated port list, move the cursor to an aggregated port and click **Delete**. The message “Are you sure you want to delete the aggregate port?” is displayed. Click **OK** to delete the aggregated port. After being deleted, the aggregated port on the panel will become available.

- Batch Deleting Aggregated Ports

In the aggregated port list, select aggregated ports to be deleted and click **Batch Del**. The message “Are you sure you want to delete the aggregate port?” is displayed. Click **OK** to delete the aggregated ports. After being deleted, the aggregated ports on the panel will become available.

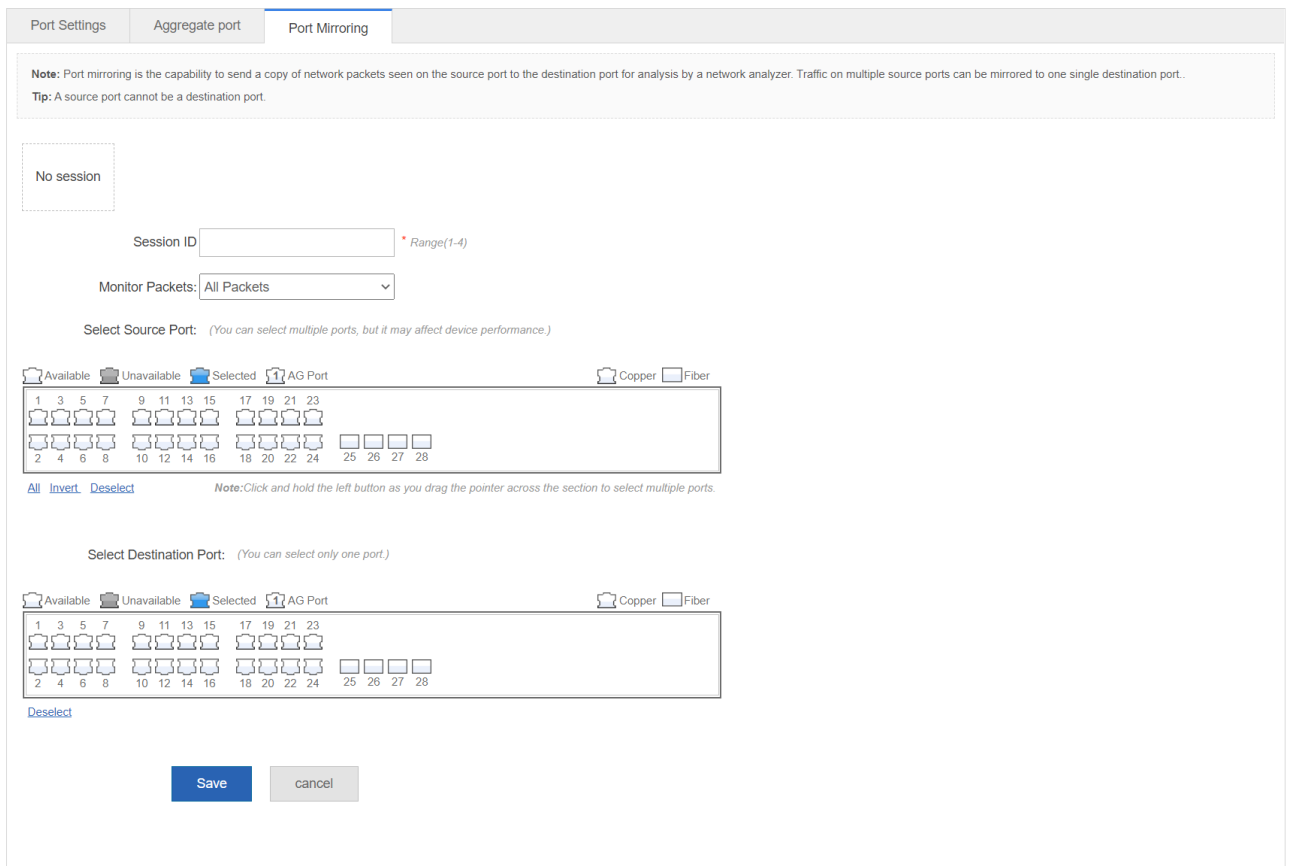
Caution

Ports enabled with ARP check, anti-ARP-spoofing, or MAC VLAN and observing ports in port mirroring cannot be added to an aggregated port, and these ports are unavailable on the panel. When you move the cursor over an unavailable port, a message is displayed, indicating that the functions are enabled on the port and the port cannot be selected.

(3) Port Mirroring

Figure 1-11 shows the **Port Mirroring** page.

Figure 1-11 Port Mirroring



The initial port mirroring page is in editing state because only one mirrored port can be configured on the Eweb. There are two panels on the interface. The port selected on the top panel will serve as the mirrored port. You can select multiple mirrored ports. You can select only one port on the bottom panel to serve as the observing port. Select or modify the port on the panel, click **Save**. The message “Configuration succeeded.” is displayed.

Note

The panel displays the current port mirroring status, and both the source and destination ports can be edited. To cancel modification of port information, click Refresh to restore the panel to the current port mirroring status.

Caution

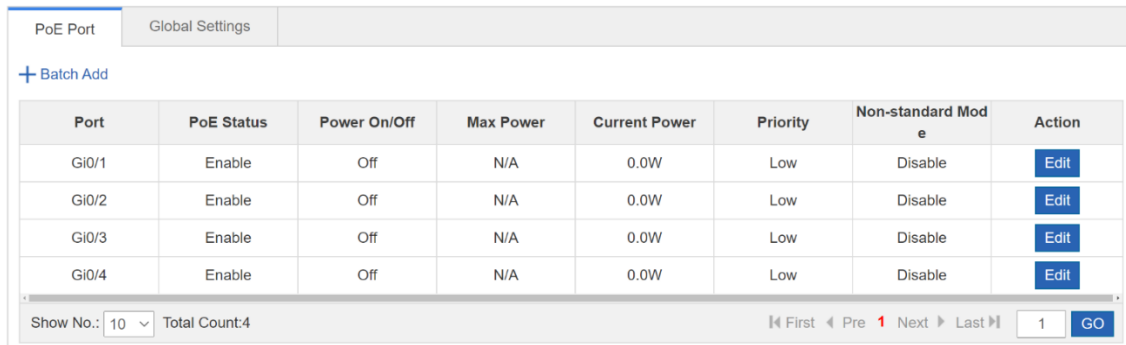
A member port of the aggregated port cannot be configured as the mirrored or observing port, and the mirrored and observing ports must be different.

4. PoE Settings

You can configure PoE on a port or in the system on the **PoE Settings** page. This page is available only for PoE-capable devices.

(1) PoE Port

Figure 1-12 PoE Port Settings



Port	PoE Status	Power On/Off	Max Power	Current Power	Priority	Non-standard Mode	Action
Gi0/1	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/2	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/3	Enable	Off	N/A	0.0W	Low	Disable	Edit
Gi0/4	Enable	Off	N/A	0.0W	Low	Disable	Edit

- **Batch Configuring Ports**

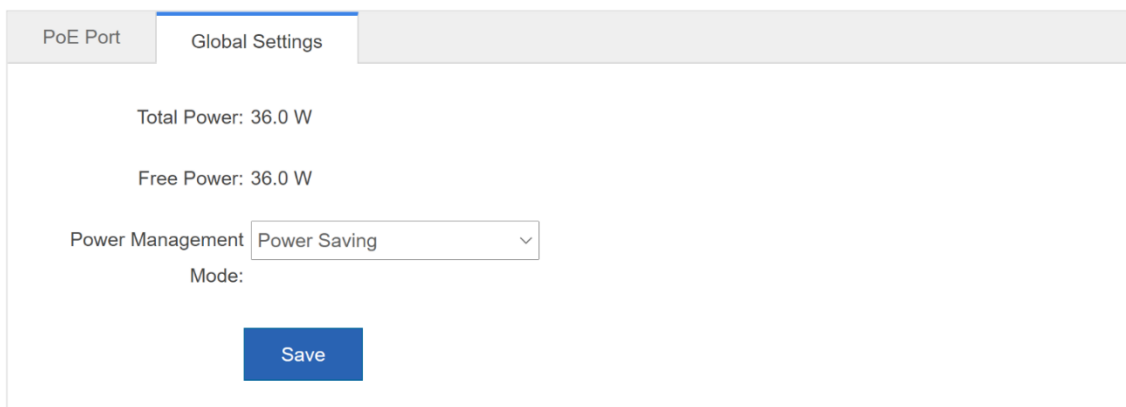
Select ports to be configured, and configure the PoE function, power supply priority, maximum power, current power, and non-standard mode. Click **Save**. The message “Configuration succeeded.” is displayed.

- **Editing a port**

Click **Edit** in the **Action** column of the port list and the port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

(2) **Global Settings**

Figure 1-13 Global Settings

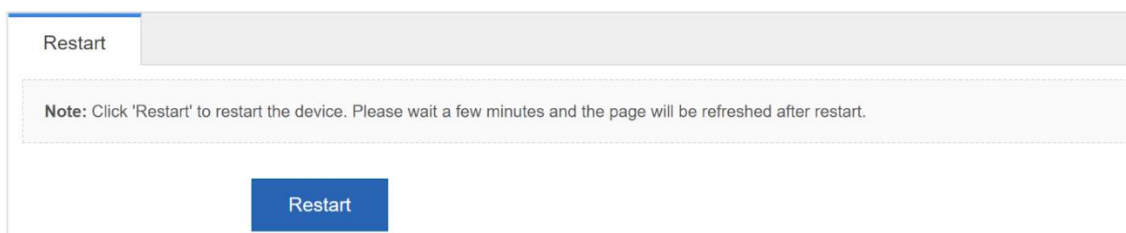


The page displays the total power, free power, and power supply management mode. Select a power supply management mode and click **Save** to configure the port.

5. Restart

Figure 1-15 shows the **Restart** page.

Figure 1-14 Restart



Click **Restart**. The message “Are you sure you want to restart the device?” is displayed. Click **OK** to restart the device. Wait for a few minutes. The page will refresh after restart.

1.3.4 Network

Click the primary menu **Network** to access the secondary menu, including **MAC Address**, **Routing**, **STP**, and **IGMP Snooping**.

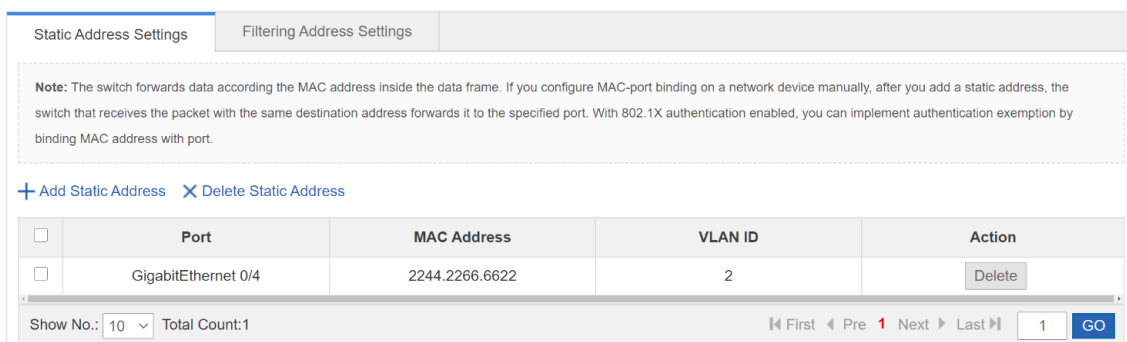
1. MAC Address

The MAC Address page includes **Static Address Settings** and **Filtering Address Settings** pages.

(1) Static Address Settings

Figure 1-16 shows the **Static Address Settings** page.

Figure 1-15 Static Address Settings



- Adding a Static Address

You must enter a MAC address and a VLAN ID and select a port to add a static address. Click **Save**. The message “Configuration Succeeded.” is displayed. The added static address is displayed in the static address list.

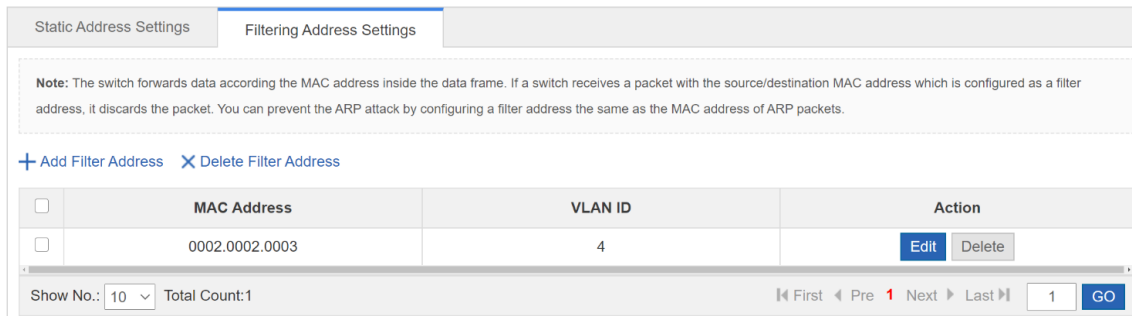
- Deleting a Static Address

- Select multiple records in the static address list and click **Delete Static Address** to batch delete the records.
- In the static address list, click **Delete** in the **Action** column for a static address. The message "Are you sure you want to delete the static address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.

(2) Filtering Address Settings

Figure 1-17 shows the **Filtering Address Settings** page.

Figure 1-16 Filtering Address Settings



- Adding a Filter Address

You must enter an MAC address, a VLAN ID to add a filter address. Click **Save** and the message “Configuration Succeeded.” is displayed. The added filter address is displayed in the filter address list.

- Editing a Filter Address

In the filter address list, click **Edit** in the **Action** column for a filter address. The address information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Filter Address

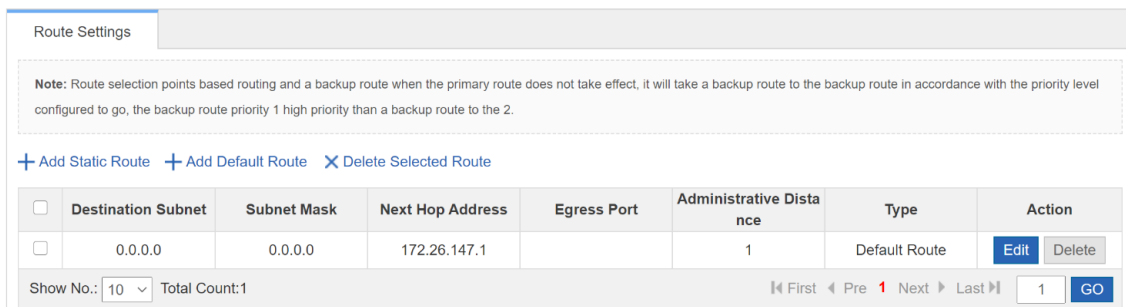
- Select multiple records in the static address list and click Delete Filter Address to batch delete the records.
- In the filter address list, click **Delete** in the **Action** column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.

2. Routing

The **Routing** page allows you to manage routes.

Figure 1-18 shows the **Routing Settings** page.

Figure 1-17 Route Settings



- Adding a Static Route

You must select an IP type and enter a destination subnet, a subnet mask, and a next-hop address to add a static address. Click **Save**. The message “Configuration Succeeded.” is displayed. The added static route is displayed in the route list.

- Editing a Route

In the route list, click **Edit** in the **Action** column for a route. Route information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Route

- Select multiple records in the route list and click **Delete Selected Route** to batch delete the records.
- In the filter address list, click **Delete** in the **Action** column for a filter address. The message "Are you sure you want to delete the filter address?" is displayed. Click **OK**. The message "Delete succeeded." is displayed.
- Adding a Default Route

Select an IP type and enter a next hop address to add a default route. Click **Save**. The message "Configuration Succeeded." is displayed. The added default route is displayed in the route list.

Note

Routes are classified into primary and backup routes. When the primary route becomes unreachable, a backup route takes over services. Backup routes are selected based on their priorities. The priority of backup route 1 is higher than that of backup route 2.

3. STP

The **STP** page allows you to configure STP global parameters, STP ports, and RLDLP.

(1) STP Global Settings

Figure 1-18 STP Global Settings

The screenshot shows the 'STP Global Settings' configuration page. At the top, there are three tabs: 'STP Global Settings', 'STP Port Settings', and 'RLDP Settings'. The 'STP Global Settings' tab is active. Below the tabs, there is a 'Global Configuration' section. It includes a toggle for 'STP' which is currently 'ON'. There are several input fields with their respective ranges and default values: Priority (8, Range(0-15), default 8), Hello Time (2, Range(1-10s), default 2), Aging Time (20, Range(6-40s), default 20), Forward Delay (15, Range(4-30s), default 15), STP Mode (MSTP), MST Name (String less than 32-byte), and MST Version (0, Range(0-65535), default 0). A 'Save' button is located below these fields. Below the 'Global Configuration' section is the 'MST Configuration' section. It contains a note: 'Note: It is recommended to disable STP before configuring an instance and enable STP again after configuration, so as to ensure the stability and convergence of network topology.' There are two buttons: '+ Add Instance' and 'X Delete Selected Instance'. Below these buttons is a table with the following columns: Instance Number, VLAN, Priority, and Action. The table contains one row: Instance Number 0, VLAN ALL, Priority 8, and Action 'Default instance. Cannot be edited.' At the bottom of the table, there is a 'Show No.' dropdown set to 10, 'Total Count: 1', and pagination controls including 'First', 'Pre', 'Next', 'Last', and a 'GO' button.

You can configure STP global parameters. When **STP Mode** is set to **MSTP**, you can configure an MST instance (MSTI).

- Adding a MSTI

The MSTI ID and VLAN range are mandatory. Other parameters are optional. Click **Save**. The message "Configuration Succeeded." is displayed. The added MSTI is displayed in the MSTI list.

- Editing a MSTI

In the MSTI list, click **Edit** in the **Action** column for an MSTI. MSTI information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

- Deleting a MSTI

- o Select multiple records in the MSTI list and click **Delete Selected Instance** to batch delete the records.
- o In the MSTI list, click **Delete** in the **Action** column for an MSTI. The message "Are you sure you want to delete the instance?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the MSTI is deleted. MSTI 0 is the default one and cannot be deleted.

(2) STP Port Settings

Figure 1-19 STP Port Settings

Port	State	Port Fast	BPDU Guard	Protection Mode	Connection Mode	Instance Cost Priority	Action
Gi0/2	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Gi0/3	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Gi0/4	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Te0/5	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit
Te0/6	Down	Disabled	Disabled	Null	Point To Point	0 0 128 64 0 128	Edit

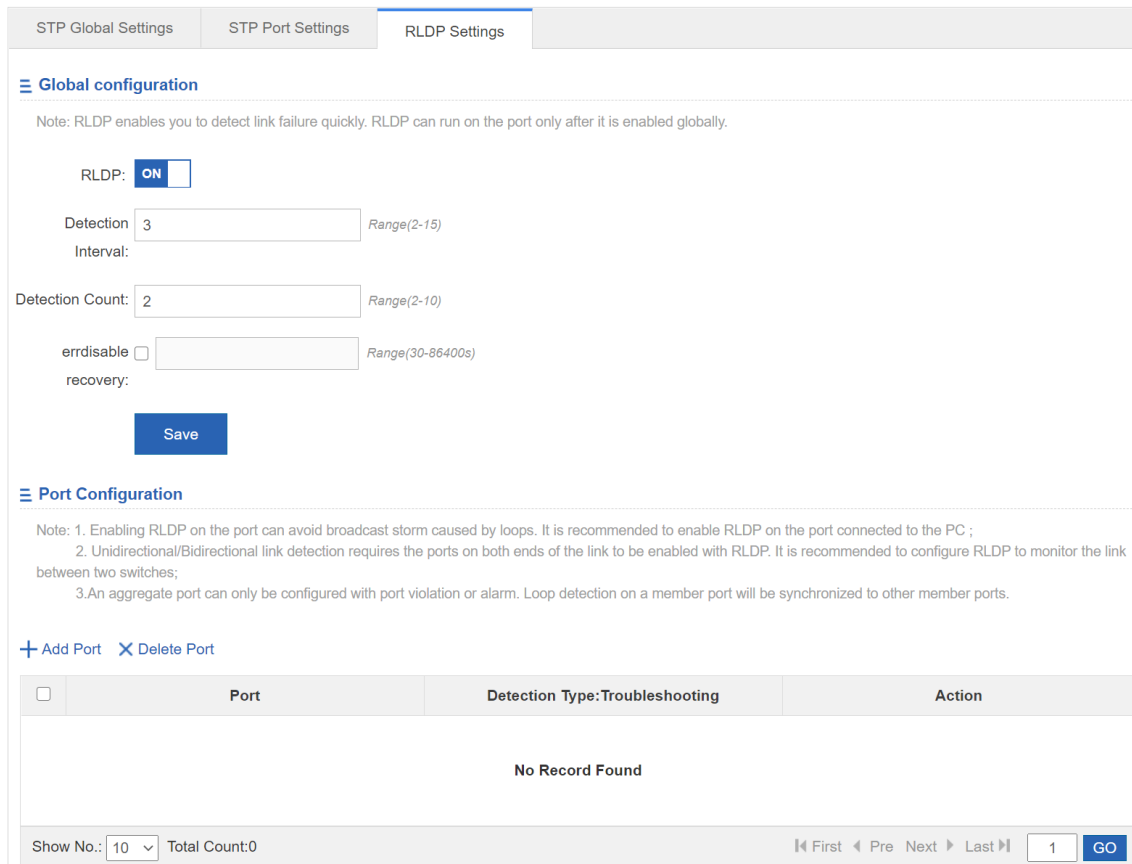
● **Batch Adding STP Ports**

Select a protection mode, a connection mode, a port priority, and whether to enable Port Fast and BPDU Guard. Select ports to be batch configured and click **Save**.

● **Editing an STP Port**

In the STP port list, click **Edit** in the **Action** column for an STP port. Port information is displayed. Edit the information and click **Save**. The message "Configuration succeeded" is displayed.

(3) RLDP Settings



(4) RLDP Global Configuration

Click **RLDP** to enable or disable the RLDP function. When the RLDP function is enabled, set a detection interval and detection count. Click **Save**. The message “Configuration Succeeded.” is displayed.

(5) RLDP Port Configuration

- Adding an RLDP-enabled Port

Select the detection modes, troubleshooting and a port. Click **Save** and the message “Save Succeeded.” is displayed., indicating that an RLDP-enabled port is added. The added RLDP-enabled port is displayed in the RLDP-enabled list.

- Editing an RLDP Port

In the RLDP-enabled port list, click **Edit** in the **Action** column for an RLDP-enabled port. Port information is displayed. Edit the information and click **Save**. The message “Save succeeded” is displayed.

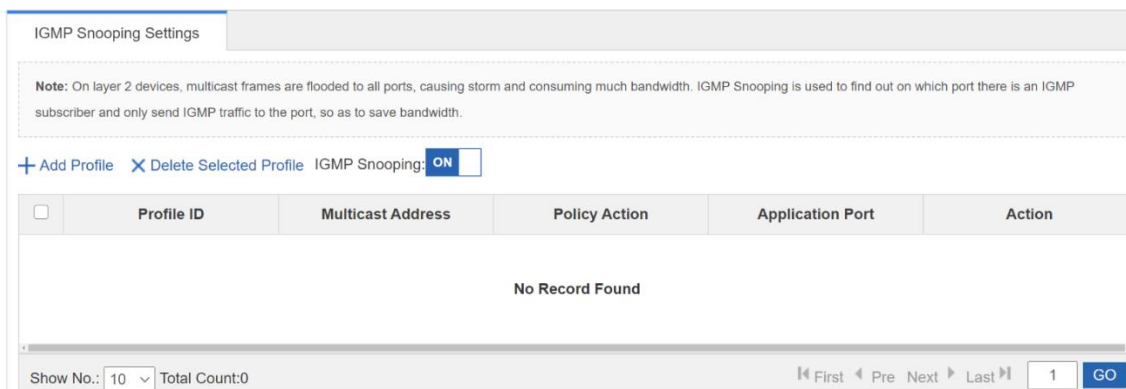
- Deleting an RLDP-enabled Port

- Select multiple records in the RLDP-enabled port list and click **Delete Port** to batch delete the records.
- In the RLDP-enabled port list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is deleted.

4. IGMP Settings

Figure 1-21 shows the **IGMP Snooping** page.

Figure 1-20 IGMP Snooping Settings



- Adding a Profile

The profile ID and multicast address range are mandatory. Other parameters are optional. Click **Save**. The message “Configuration Succeeded.” is displayed. The added profile is displayed in the profile list.

- Editing a Profile

In the profile list, click **Edit** in the **Action** column for a profile. Profile information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Profile

- Select multiple records in the profile list and click **Delete Selected Profile** to batch delete the records.
- In the profile list, click **Delete** in the **Action** column for a profile. The message "Are you sure you want to delete the profile?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the profile is deleted.

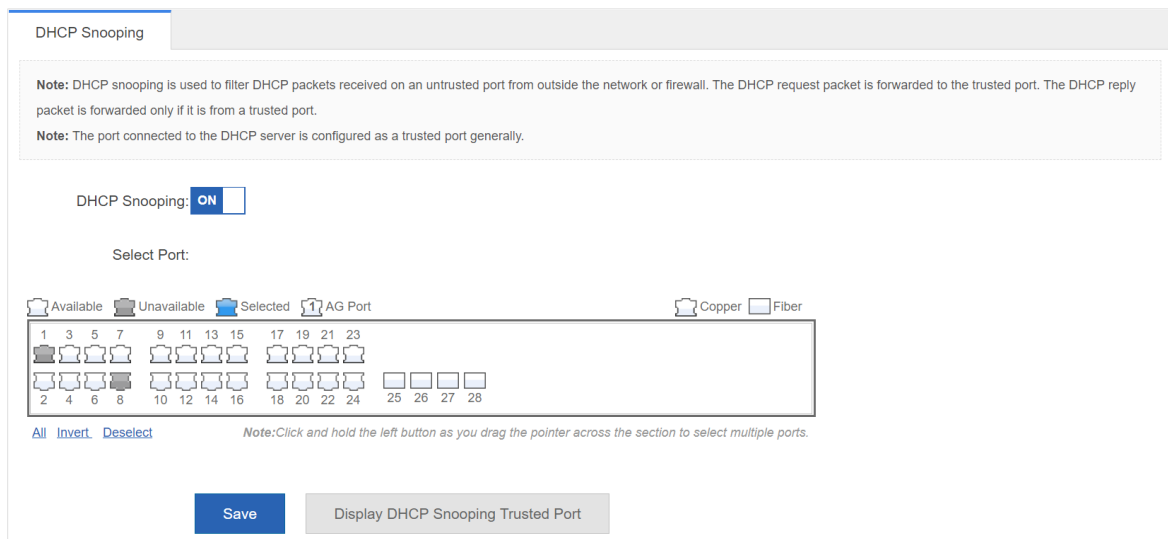
1.3.5 Security

Click the primary menu **Security** to access the secondary menu, including **DHCP Snooping**, **Gateway Anti-ARP-Snooping**, **IP Source Guard**, **NFPP** and **Storm Control**.

1. DHCP Snooping

Figure 1-25 shows the **DHCP Snooping** page.

Figure 1-21 DHCP Snooping



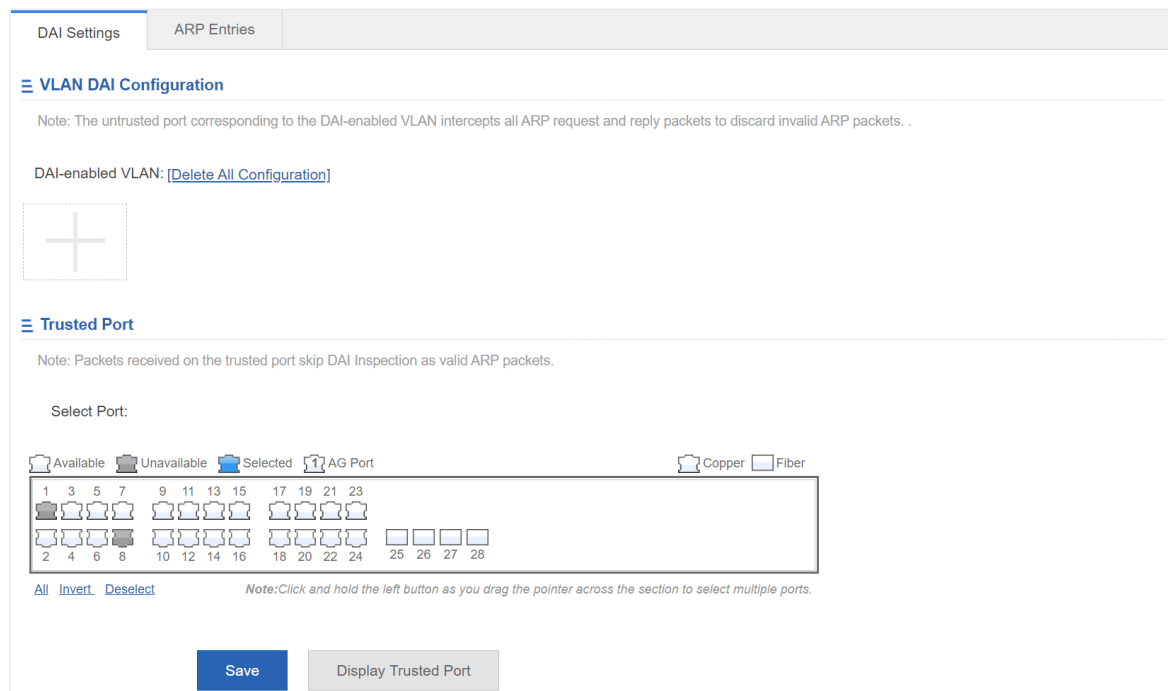
The port connected to a DHCP server needs to be configured as a DHCP trusted port. The DHCP server connected to a non-trusted port cannot work properly. The selected port is configured as a DHCP trusted port. You can select ports on the panel and click **Save**.

2. Gateway Anti-ARP-Snooping

The Gateway Anti-ARP-Snooping page allows you to configure DAI settings and ARP entries.

(1) DAI Settings

Figure 1-22 DAI Settings



- VLAN DAI Settings

Click the add icon to add a VLAN where DAI is enabled.

- DAI Trusted Port

Select a port on the panel to enable the DAI trusted port.

Note

The panel displays DAI trusted ports and the ports can be edited. To cancel modification of a port, click **Display Trusted Port** to display current DAI trusted ports on the panel.

Caution

The ARP check function cannot be enabled on DHCP snooping trusted ports.

(2) ARP Entries

Figure 1-23 ARP Entries

IP	MAC	Type	Action
10.110.69.1	8005.889b.1447	Dynamic Binding	Dynamic Binding>>Static Binding
10.110.69.3	0074.9c03.f1ab	Dynamic Binding	Dynamic Binding>>Static Binding
10.110.69.31	00d0.f822.3546	Dynamic Binding	Dynamic Binding>>Static Binding
10.110.69.99	0000.f823.0111	Local ARP Entry	Dynamic Binding>>Static Binding
10.110.69.111	1082.3d95.47ef	Dynamic Binding	Dynamic Binding>>Static Binding

- Dynamic binding >> static binding
 - Select multiple dynamic binding entries in the ARP entry list and click **Dynamic Binding >> Static Binding**.
 - In the ARP entry list, click **Dynamic Binding >> Static Binding** in the **Action** column for an ARP entry. The message "Configuration succeeded." is displayed.
- Removing a Static Bindings
 - Select multiple static binding entries in the ARP entry list and click **Remove Static Binding** to batch remove static bindings.
 - In the ARP entry list, click **Remove Static Binding** in the **Action** column for a static binding entry. The message "Configuration succeeded." is displayed.
- Manual binding

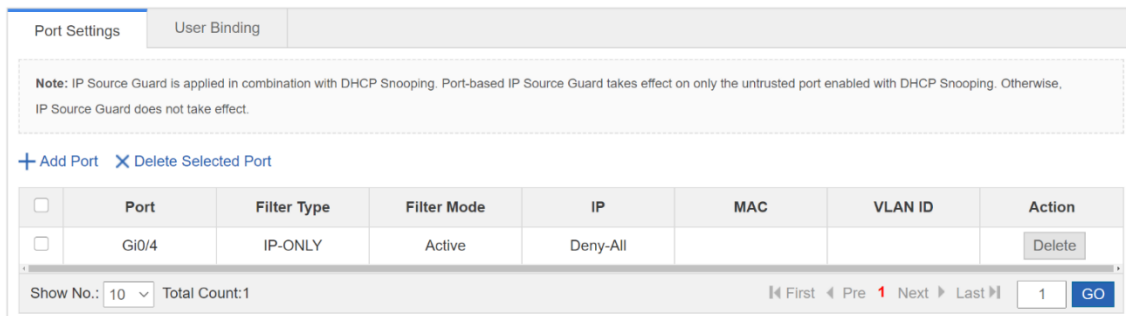
You must enter an IP address and a MAC address to add a static binding entry. Click **Save**. The message "Configuration Succeeded." is displayed. The added static binding entry is displayed in the port filter list.

3. IP Source Guard

The **IP Source Guard** page allows you to configure ports and bind users.

(1) Port Settings

Figure 1-24 Port Settings



- Adding a Port Enabled with IP Source Guard

Click **Add Port** and select a filter type and a port to add a port enabled with IP source guard. Click **Save**. The message “Configuration Succeeded.” is displayed. The added port is displayed in the list of ports enabled with IP source guard.

- Editing a Port Enabled with IP Source Guard

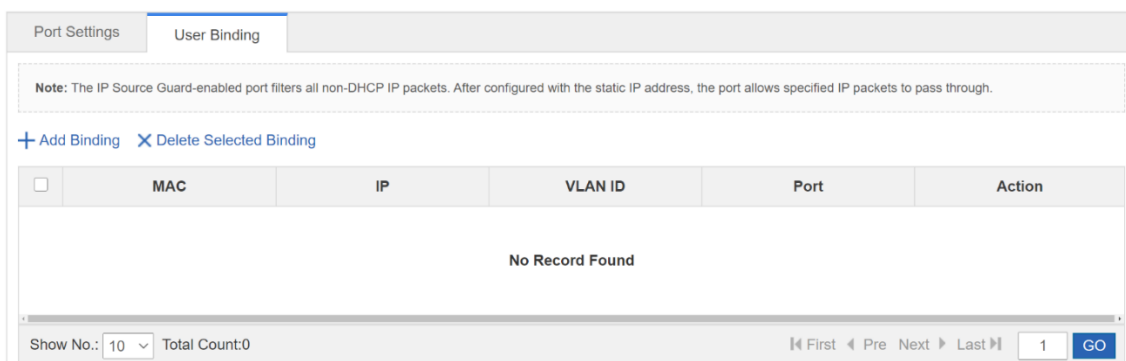
In the list of ports enabled with IP source guard, click **Edit** in the **Action** column for a port. Port information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Port Enabled with IP Source Guard

- Select multiple records in the list of ports enabled with IP source guard and click **Delete Selected Port** to batch delete records.
- In the list of ports enabled with IP source guard, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port is displayed.

(2) User Binding

Figure 1-25 User Binding



- Adding a User Binding

You must enter a MAC address, an IP address, and a VLAN ID to add a user binding. Click **Save**. The message “Configuration Succeeded.” is displayed. The added binding is displayed in the user binding list.

- Editing a User Binding

In the user binding list, click **Edit** in the **Action** column for a user binding. Binding information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is deleted.

- Deleting a User Binding

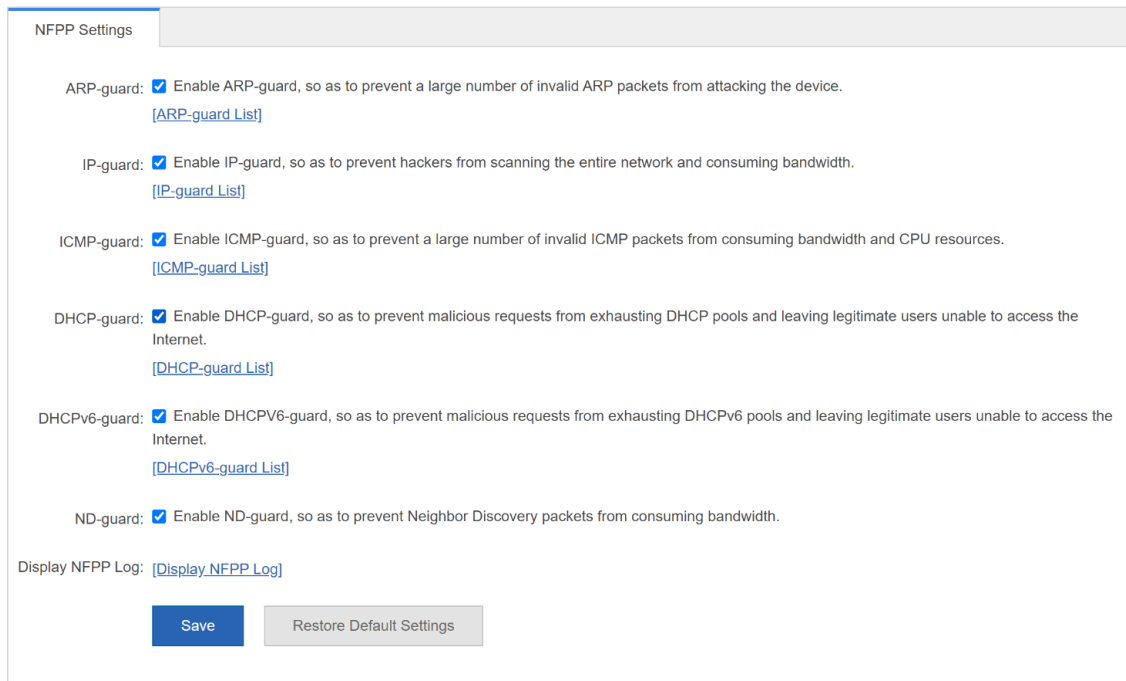
- Select multiple records in the user binding list and click **Delete Selected Binding** to batch delete records.

- In the user binding list, click **Delete** in the **Action** column for a port. The message "Are you sure you want to delete the binding?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the binding is displayed.

4. NFPP

Figure 1-34 shows the **NFPP** page.

Figure 1-26 NFPP

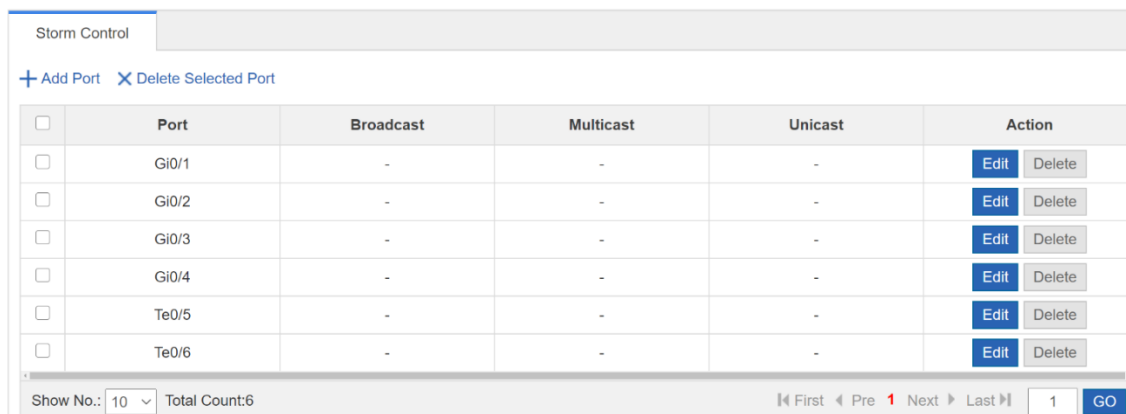


You can enable or disable each attack guard function and click **Save**. The message "Configuration succeeded" is displayed. To restore default settings, click **Restore Default Settings**.

5. Storm Control

Figure 1-35 shows the **Storm Control** page.

Figure 1-27 Figure 1-35 Storm Control



- Adding a Port Enabled with Storm Control

You must enter one of the broadcast address, unicast address, and multicast address to add a port enabled with storm control port. Click **Save**. The message “Configuration Succeeded.” is displayed. The added port is displayed in the list of ports enabled with storm control.

- Editing a Port Enabled with Storm Control

In the list of ports enabled with storm control, click **Edit** in the **Action** column for a port. Information about the port enabled with storm control is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting a Port Enabled with Storm Control

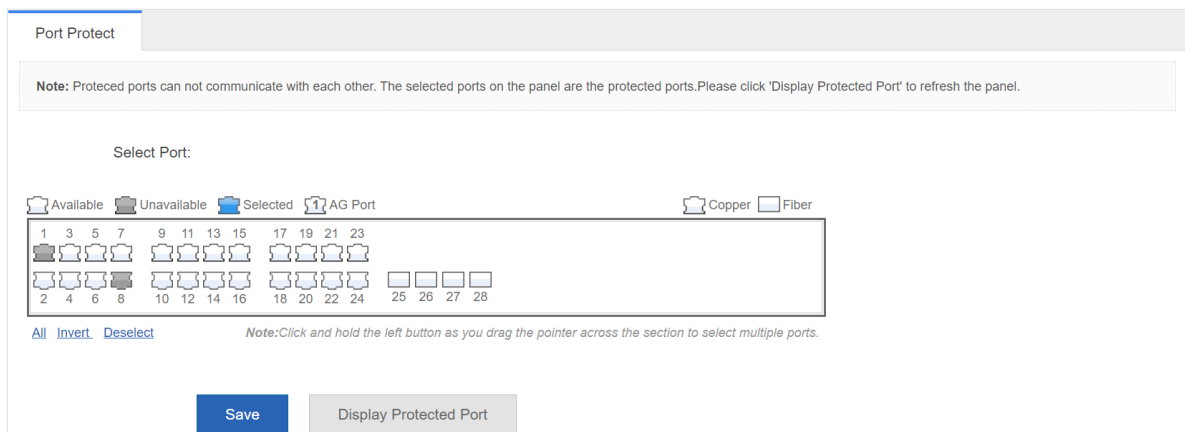
- Select multiple records in the list of ports enabled with storm control and click **Delete Selected Port** to batch delete records.
- In the list of ports enabled with storm control, click **Delete** in the Action column for a port. The message "Are you sure you want to delete the storm control port?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the port enabled with storm control is deleted.

1.3.6 Advanced

1. Port Protection

Figure 1-36 shows the **Port Protect** page.

Figure 1-28 Port Protect



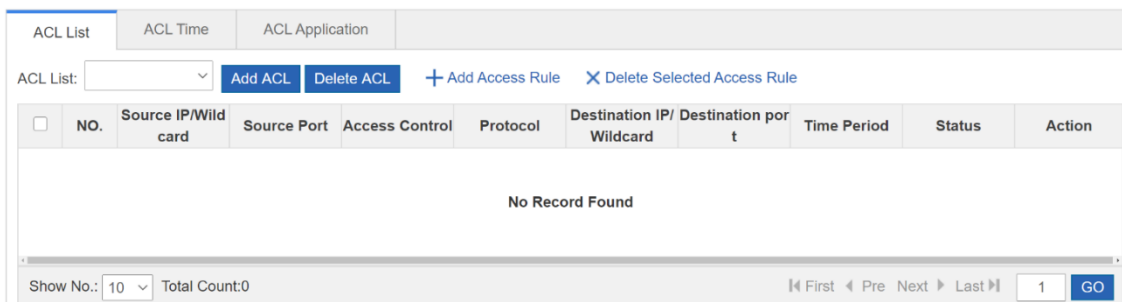
Select a port on the panel to be configured as a protected port. Click **Save**. The message “Configuration Succeeded.” is displayed.

2. ACL

(1) ACL List

Figure 1-40 shows the **ACL List** page.

Figure 1-29 ACL List



- Adding an ACL

Click **Add ACL** and configure the ACL to be added. You must enter an ACL. Click **Save**. The message “Configuration succeeded.” is displayed. The added ACL is displayed in the ACL list.

- Deleting an ACL

In the ACL list, select the ACL to be deleted and click **Delete ACL**. The message "Delete succeeded." is displayed.

- Adding an ACL Rule

Select an ACL type, a protocol, and a time period, and configure an IP address to add an ACL rule. Click **Save**. The message “Configuration succeeded.” is displayed. The added ACL rule is displayed in the ACL rule list.

- Editing an ACL Rule

In the ACL rule list, click **Edit** in the **Action** column for a rule. ACL rule information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting an ACL Rule

- Select multiple records in the ACL rule list and click **Delete Selected Access Rule** to batch delete records.
- In the ACL rule list, click **Delete** in the **Action** column for a rule. The message "Are you sure you want to delete the rule?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the rule is deleted.

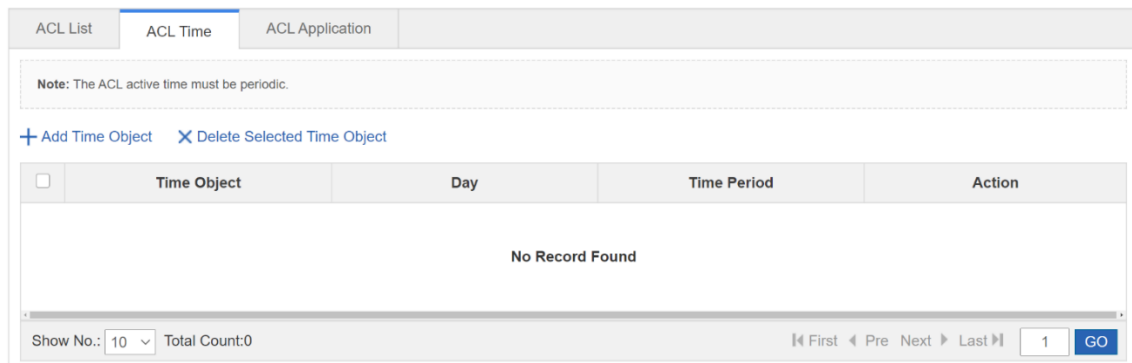
- Moving an ACL Rule

Enter the ID of an ACL rule to be moved and click **Move**. The message “Configuration succeeded.” is displayed.

(2) ACL Time

Figure 1-41 shows the **ACL Time** page.

Figure 1-30 ACL Time



- Adding ACL Time

Enter the time object name and select a time period to add an ACL time. Click **Save**. The message “Configuration succeeded.” is displayed. The added ACL time is displayed in the ACL time list.

- Editing ACL Time

In the ACL time list, click **Edit** in the **Action** column for an ACL time. ACL time information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

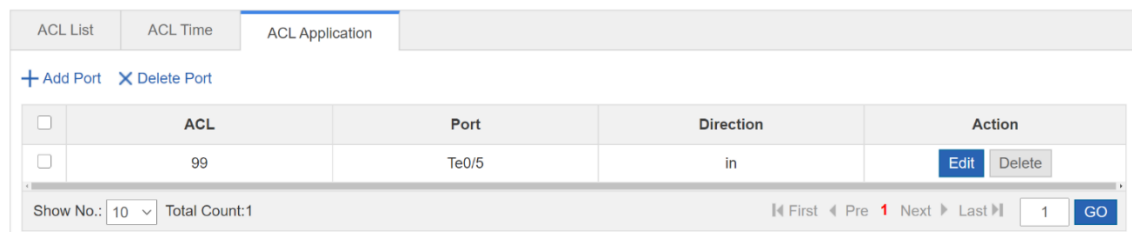
- Deleting ACL Time

Select multiple records in the ACL time list and click **Delete Selected Time Object** to batch delete records.

(3) ACL Application

Figure 1-42 shows the **ACL Application** page.

Figure 1-31 ACL Application



- Adding an Applied ACL

Select an ACL list, a filter direction and a port and click **Save**. The message “Configuration succeeded.” is displayed. The added ACL applied to a port is displayed in the applied ACL list.

- Editing an Applied ACL

In the applied ACL list, click **Edit** in the **Action** column. Applied ACL information is displayed. Edit the information and click **Save**. The message “Configuration succeeded” is displayed.

- Deleting an Applied ACL

- Select multiple records in the applied ACL list and click **Delete Port** to batch delete records.

- In the applied ACL list, click **Delete** in the **Action** column for an applied ACL. The message "Are you sure you want to delete the item?" is displayed. Click **OK**. The message "Delete succeeded." is displayed, indicating that the applied ACL is deleted.

1.3.7 System

The **System** page allows you to configure system settings, upload the system, configure system logging, CWMP, and network detection, and use the web console.

1. Settings

The **Settings** page includes **System Time**, **Password**, **Reset**, **Enhancement**, **SNMP** and **DNS**.

(1) System Time

Figure 1-46 shows the **System Time** page.

Figure 1-32 System Time

- System Time

The page displays the current system time. You can set the system time manually or click **Automatically synchronize with an Internet time server**.

Select either of the two methods to set the system time. Click **Save**. The message “Configuration succeeded.” is displayed.

(2) Password

Figure 1-47 shows the **Password** page.

Figure 1-33 Password

- Changing the Web Management Password

You need to enter the old password and enter a new password twice to change the web management password. If the input old password is incorrect, the message "Incorrect old password" in red font is displayed. You are required to enter the correct old password and click **Save** to complete the password change.

Note

The enable password is changed by default when the password of the Eweb is changed.

- Changing the Telnet Authentication Password

To change the telnet password, you do not need to enter the old password but need to enter a new password twice. Other operations are the same as those of changing the password of the super administrator.

(3) Reset

Figure 1-48 shows the **Reset** page.

Figure 1-34 Reset

The screenshot shows the 'Reset' page in the Eweb configuration interface. The page has a navigation bar with tabs: System Time, Password, Reset (selected), Enhancement, SNMP, and DNS. Below the navigation bar, there are three main sections: 'Restore Factory Settings', 'Display Current Configuration', and 'Import/Export Configuration'. The 'Restore Factory Settings' section contains a blue button labeled 'Restore Factory Settings'. The 'Display Current Configuration' section contains a large empty text area. The 'Import/Export Configuration' section contains a 'File Name:' input field, a 'File...' button, an 'Import' button, and an 'Export Current Configuration' button. A note is present above the 'Import/Export Configuration' section.

- Import/Export Configuration

Import the configuration to modify the device configuration and restart the device to make the configuration take effect. Export the current configuration for backup.

- Restore Factory Settings

Click **Restore Factory Settings** to clear the configuration and restore factory settings.

(4) Enhancement

Figure 1-49 shows the **Enhancement** page.

Figure 1-35 Enhancement

The screenshot shows the 'Enhancement' configuration page. At the top, there are navigation tabs: System Time, Password, Reset, Enhancement (active), SNMP, and DNS. Below the tabs is a section titled 'Basic Information'. It contains the following fields and options:

- Web Access Port:** A text input field containing '443'. A red asterisk and a note '(Range:443,1025-65535)' are to its right.
- Login Timeout:** A dropdown menu showing '10 min'.
- Device Location:** An empty text input field.
- Access Redirection:** A checkbox labeled 'HTTP Redirection to HTTPS'. To its right is a note: 'In NAT scenario, redirection may cause HTTP access failure.'

A blue 'Save' button is located at the bottom center of the configuration area.

You must set a web access port. The login timeout and device location are optional. Click **Save**. The message “Configuration succeeded.” is displayed.

(5) SNMP

Figure 1-50 shows the **SNMP** page.

Figure 1-36 SNMP

The screenshot shows the 'SNMP' configuration page. At the top, there are navigation tabs: System Time, Password, Reset, Enhancement, SNMP (active), and DNS. Below the tabs is a note: 'Note: Either SNMPv2 or SNMPv3 is supported'. The configuration area includes:

- SNMP Version:** Radio buttons for 'v2' (selected) and 'v3'.
- Device Location:** An empty text input field.
- SNMP Community:** An empty text input field with a red asterisk to its right.
- Trap Community:** An empty text input field. A note to its right says: 'The Trap Community must be the same as the SNMP Community.'
- Trap Recipient Address:** A large empty text area. A note to its right says: '* You can configure up to 9 Trap recipients. Please use ',' or press the Enter key to separate addresses.'

A blue 'Save' button is located at the bottom center of the configuration area.

Select an SNMP version. The device location, SNMP community, and trap recipient address are mandatory, and other parameters are optional. Click **Save**. The message “Configuration succeeded.” is displayed.

(6) DNS

Figure 1-51 shows the **DNS** page.

Figure 1-37 DNS

The screenshot shows the 'DNS' configuration page. At the top, there are navigation tabs: System Time, Password, Reset, Enhancement, SNMP, and DNS (active). The configuration area contains:

- DNS Server 1:** A text input field containing '114.114.114.114' with a blue plus sign to its right.

A blue 'Save' button is located at the bottom center of the configuration area.

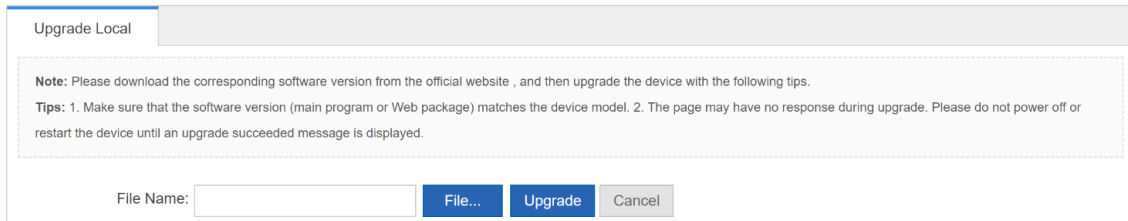
Enter a DNS server address. Click **Save**. The message “Configuration succeeded.” is displayed.

2. Upgrade

(1) Local Upgrade

The figure below shows the **Upgrade Local** page.

Figure 1-38 Upgrade Local



Click **File**, select the locally saved bin file, and then click **Upgrade** to perform local upgrade.

3. System Logging

The **System Logging** page includes **Log Server Settings** and **Display System Log**

(1) Log Server Settings

Figure 1-53 shows the **Log Server Settings** page.

Figure 1-39 Log Server Settings

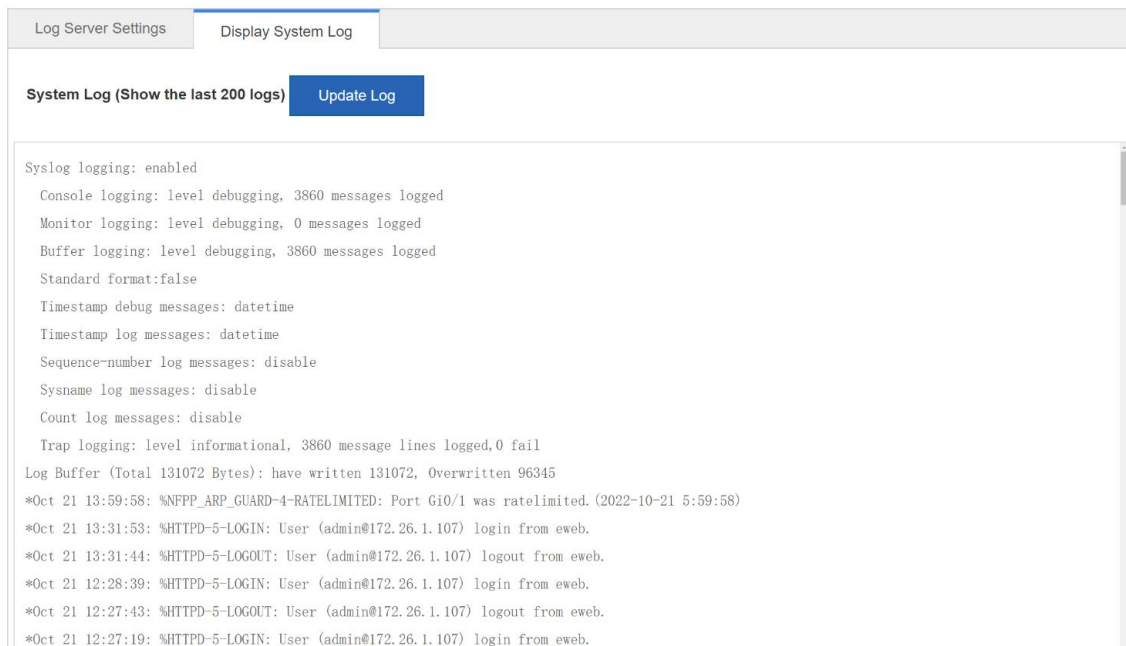


Enter a server IP address and select a log severity. Then the device will send system logs to the corresponding server.

(2) Display System Log

Figure 1-54 shows the **Display System Log** page.

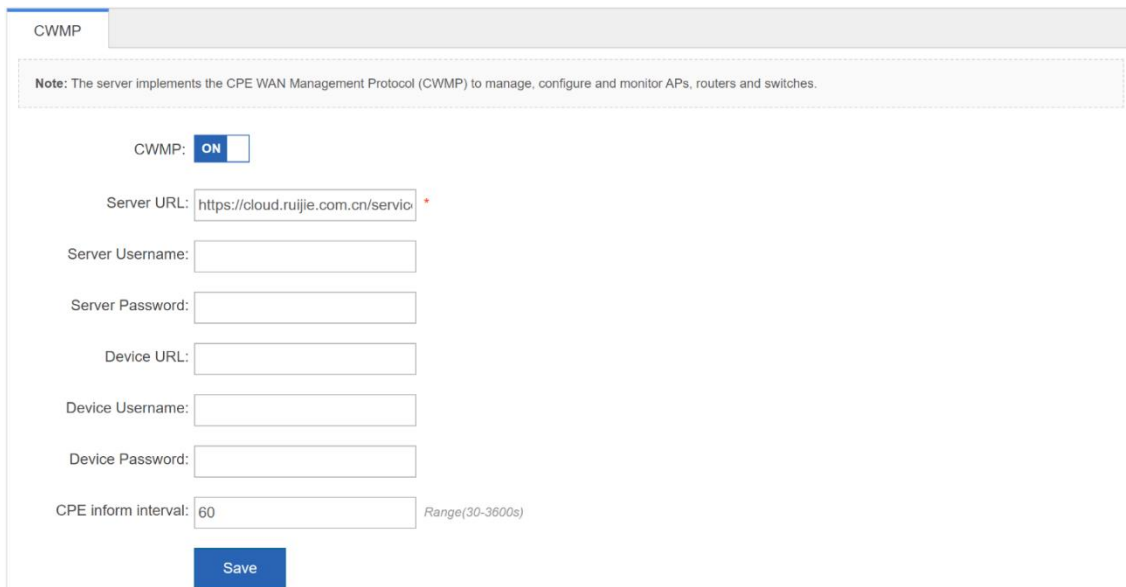
Figure 1-40 Display System Log



The text box displays current system logs. Click **Update Log** to update logs.

4. CWMP

The **CWMP** page allows you to view and configure CWMP.



Enable or disable CWMP. You can configure the server URL, server name, server password, device URL, device name, device password, and device connection interval.

5. Detection

The **Detection** page includes **Ping**, **Tracert** and **Cable Detection**.

(1) Ping

Figure 1-55 shows the **Ping** page.

Figure 1-41 Ping

Enter the destination IP and other parameters, and click **Detect**. Wait for a few minutes. The text box will display the detected results.

(2) Tracert

Figure 1-56 shows the **Tracert** page.

Figure 1-42 Tracert

The steps of tracert test are the same as those of the ping test. Enter the destination IP and other parameters, and click **Detect**. Wait for a few minutes. The text box will display the detected results.

(3) Cable Detection

Figure 1-57 shows the **Cable Detection** page.

Figure 1-43 Cable Detection

Select a port on the panel and click **Detect**. Wait for a few minutes. Test results will be displayed below **Detect**.

Figure 1-44 Test Results

The screenshot shows the 'Cable Detection' tab in a web-based configuration tool. At the top, there are tabs for 'Ping', 'Tracert', and 'Cable Detection'. A note states: 'Note: Fast port detects only A and B two pairs of core, length error 10 m'. Below the note, there is a 'Select Port:' section with icons for 'Available', 'Unavailable', 'Selected', and 'AG Port'. There are also checkboxes for 'Copper' and 'Fiber'. A grid of 28 port icons is shown, with ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23 in the first row, and ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 25, 26, 27, and 28 in the second row. Port 13 is selected. A 'Detect' button is located below the grid. Below the 'Detect' button, the 'Test Results:' section contains a table with the following data:

Port:(A / B / C / D represent four cable pairs)	State	Meters
Gi0/13:A	Open	0
Gi0/13:B	Open	0
Gi0/13:C	Open	0
Gi0/13:D	Open	0

6. Web Console

The page simulates the CLI console. Enter CLI commands in the input box, and press Enter or click **Send** to input commands. The page supports tab completion and ? command.

Figure 1-45

The screenshot shows the 'Web Cli' interface. At the top, there is a 'Web Cli' tab. Below it, the 'Console Output:' section displays the following text: 'SF2910-JR-230#aaa', '% Unknown command.', and 'SF2910-JR-230#'. To the right of the console output, there is a 'Background Color:' label with three color selection boxes: black, blue, and red. Below the console output, there is a 'Command Input:' section with a text input box containing 'show interface ?'. To the right of the input box are 'Send' and 'Clear Screen' buttons. A dropdown menu is open below the input box, showing the following options: 'AggregatePort', 'GigabitEthernet', 'Loopback', 'Null', and 'TenGigabitEthernet'.