Reyee ES_NBS Series Switch

Cookbook

Document Version: V1.2

Date: 2022.11.25

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are 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.

Note

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

Instruction

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. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.

The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.

The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Contents

1 Product Introduction

1.1 Reyee ES200 Switch

Ruijie Reyee smart surveillance switches offer a variety of port options to meet the needs of video surveillance networks of different scales. Ruijie Reyee smart surveillance switches support full-power PoE output to ensure that all cameras can be powered simultaneously when connected to the switch at maximum capacity. In addition, Ruijie Real-easy Series smart surveillance switches provide simple and easy-to-use management features while offering plug and play with default factory configuration, which can quickly locate the surveillance network faults, initiate PoE port restart, perform VLAN configuration, etc. Ruijie Cloud app and Ruijie Cloud platform remote management is also supported, making the operation and maintenance of the surveillance network easier and more convenient, while reducing operation and maintenance costs.

1.1.1 Product List

Model	10/100 Base-T Auto-sensing Ethernet Port	10/100/1000 Base-T Auto-sensing Ethernet Port	1000Base-X SFP Port	Console Port
RG-ES205GC-P	N/A	5 (Ports 1-4 support PoE+/PoE)	N/A	N/A
RG-ES209GC-P	N/A	9 (Ports 1-8 support PoE+/PoE)	N/A	N/A
RG-ES218GC-P	N/A	16 (Support PoE+/PoE)	2	N/A
RG-ES226GC-P	N/A	24 (Support PoE+/PoE)	2	N/A

Model	10/100 Base-T Auto-sensing Ethernet Port	10/100/1000 Base-T Auto-sensing Ethernet Port	1000Base-X SFP Port	Console Port
RG-ES224GC	N/A	24	N/A	N/A
RG-ES216GC	N/A	16	N/A	N/A

The SPF ports cannot be downward compatible with 100Base-FX.

1000Base-T is compatible with 100Base-TX and 10Base-T in the downlink direction.

1.1.2 LED Indicator

LED	State	Meaning
System status LED	Off	The switch is not receiving power.
	Blinking green	The PoE power exceeds the power of the entire device (370 W). The new connected PD cannot be powered up due to insufficient power. The switching function is operational.
	Solid green	The switch is operational.
RJ45 port PoE status LED	Off	PoE is not enabled.
	Solid green	PoE is enabled. The port is operational.
	Blinking green	Indicates PoE overload.
1000Mbps RJ-45 port status LED	Off	The port is not connected.
	Solid green	The port is connected at 10/100/1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
SFP port status LED	Off	The port is not connected.
	Solid green	The port is connected at 1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 1000 Mbps.

1.1.3 Button

Botton	Description

Port mode LED Switch-Over button	When the button is turned to the left position (Mode 1), the LED indicates the switching status of the port: when the LED is solid green, it indicates that the link is up; when the LED blinks green, data is being transmitted or received. When the button is turned to the right position (Mode 2), the LED indicates the PoE status of ports: when the LED is solid green, it indicates that the PoE-supported ports are supplying power; when the LED blinks green, the power of the ports is overloaded.
System reset button	The switch reboots after the reset button is pressed for less than 2 seconds. The switch restores the default factory settings after the reset button is pressed for more than 5 seconds (until the status LED blinks).

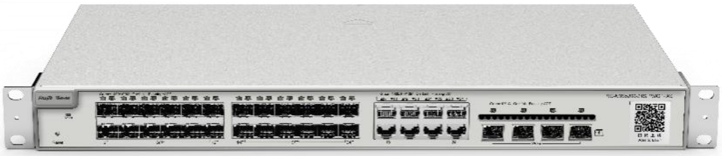
1.2 Reyee NBS Switch

Reyee RG-NBS3100 series of managed switches are Reyee's 4 switches tailored for SME customer applications, which can meet the different levels of network access needs of SME customers. Covering basic VLAN division and advanced security features such as ACL,etc. The model with the suffix '-P' is a model that supports PoE output, and can meet the PoE power supply requirements of wireless APs, digital cameras and other devices in various occasions.

RG-NBS3200 series switch is a new generation of high-performance, strong security and integrated multi-service layer 2 Ethernet switch launched by Reyee. This series of switches adopts an efficient hardware architecture design, providing larger entry specifications and faster Hardware processing performance, more convenient operation experience. The RG-NBS3200 series provides flexible Gigabit access to 10 Gigabit uplink ports. The entire series of switches all have 4-port 10 Gigabit optical and high-performance port uplink capabilities.

Ruijie RG-NBS5100&5200 Series Switches are the next-generation high-performance, high-security and multi-service Layer 3 Ethernet switches. Adopting an efficient hardware architecture design, this switch series provides larger MAC address table size, faster hardware processing performance, and more convenient operating experience. RG-NBS5100 series provides Gigabit access and Gigabit uplink, while RG-NBS5200 series provides Gigabit access and 10G uplink ports. Every switch of this series offers 4 fixed 10G fiber ports with high-performance uplink capability.

RG-NBS5100&5200 series switches provide comprehensive end-to-end QoS as well as flexible and rich security settings for small and medium-sized networks at an extremely high price-performance ratio to meet the needs of high-speed, secure and smart enterprise networks.



1.2.1 Product List

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Supply
RG-NBS3100-24GT4SFP	24	4	N/A	N/A	Single
RG-NBS3100-24GT4SFP-P	24 (Support PoE+)	4	N/A	N/A	Single
RG-NBS3100-8GT2SFP	8	2	N/A	N/A	Power adapter
RG-NBS3100-8GT2SFP-P	8 (Support PoE+)	2	N/A	N/A	Single
RG-NBS3200-24GT4XS	24	N/A	4	N/A	Single
RG-NBS3200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Single
RG-NBS3200-24GT4XS-P	24 (Support PoE+)	N/A	4	N/A	Single
RG-NBS3200-48GT4XS	48	N/A	4	N/A	Single
RG-NBS3200-48GT4XS-P	48 (Support PoE+)	N/A	4	N/A	Single

RG-NBS5100-24GT4SFP	24	4	N/A	N/A	Single
RG-NBS5100-48GT4SFP	48	4	N/A	N/A	Single
RG-NBS5200-24GT4XS	24	N/A	4	N/A	Single
RG-NBS5200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Single
RG-NBS5200-48GT4XS	48	N/A	4	N/A	Single

SFP port is downward compatible with 100Base-FX.

1000Base-T is downward compatible with 100Base-TX and 10Base-T.

Combo port consists of one 1000Base-X SFP port and one 10/100/1000Base-T Ethernet port. That is, only one port of them is available at a particular time.

1.2.2 LED Indicator

LED	State	Meaning
System status LED	Off	The switch is not receiving power.
	Blinking green (0.5 Hz)	The switch is running, but the alarm of insufficient PoE power prompts.
	Blinking green (10Hz)	The switch is being upgraded or initialized.
	Solid green	The switch is connected to Ruijie Cloud.
10/100/1000Base-T Ethernet port status LED	Off	The port is not connected.
	Solid green	The port is connected at 10/100/1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
RJ45 port PoE status LED	Off	PoE is not enabled.
	Solid green	PoE is enabled. The port is operational.
	Blinking green	The port has a PoE fault of overload.
SFP port status LED	Off	The port is not connected.
	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.

SFP+ port status LED	Off	The port is not connected.
	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.

1.2.3 Button

Botton	Description
PoE mode switch-over button	Press PoE Mode Switch-Over Button for above 3 seconds to switch the display mode between PoE mode and port rate mode.
Reset button	The switch reboots after the reset button is pressed for less than 2 seconds. The switch restores the default factory settings after the reset button is pressed for more than 5 seconds (until the status LED blinks).

2 Device Management

2.1 Logging in

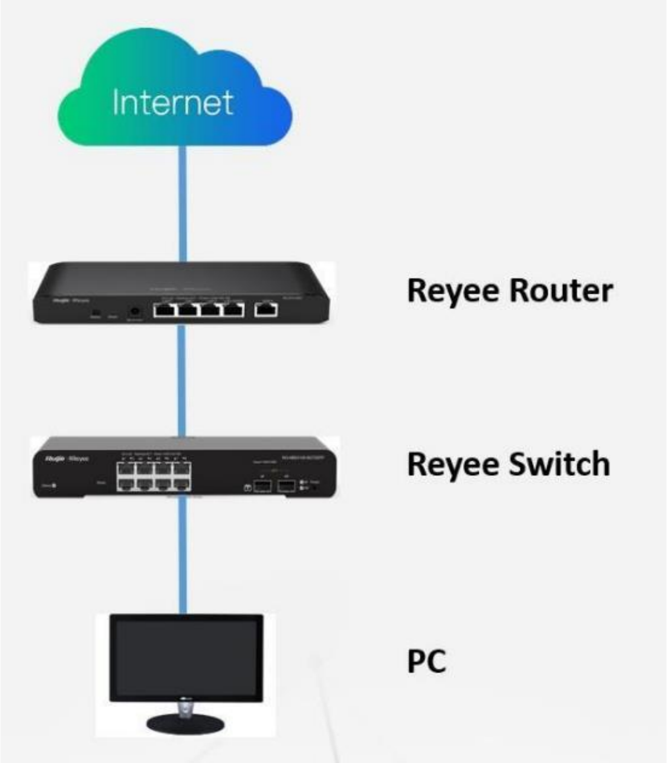
Web is a Web-based network management system used to manage or configure devices. You can access eWeb via browsers such as Google Chrome.Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

The Reyee managed switches not only support Web interface management, but also support life-time-free Ruijie Cloud App and Ruijie Cloud platform remote management. Users can view the network status, modify the configuration, and troubleshooting at home.

2.1.1 Case Demonstration

Network Topology

As shown in the figure below, you can access the eWeb management system of an access or aggregation switch via PC browser to manage and configure the device.

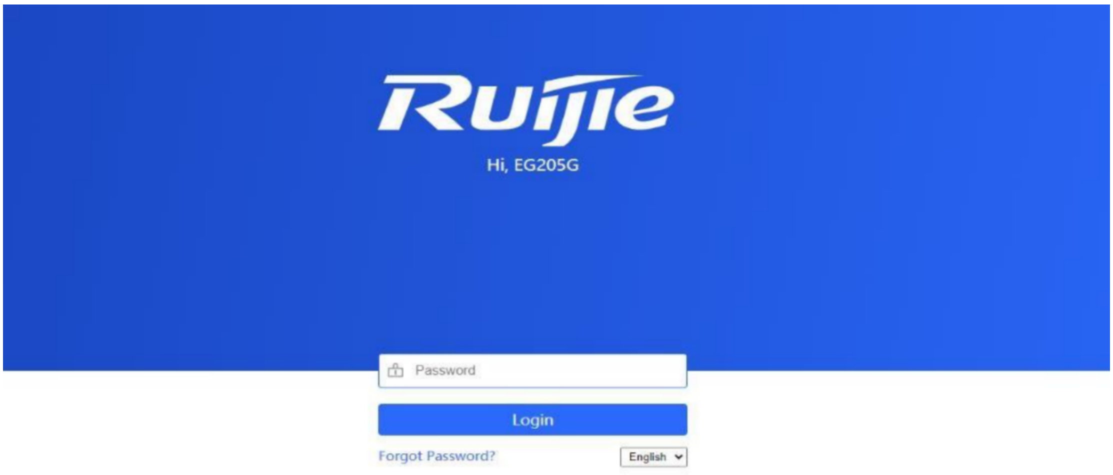


Set PC’s IP assignment mode to obtain the IP address automatically.

Visit http://192.168.110.1 by Chrome browser.

Enter the password on the login page and click “Login”.

Default Password: admin



For the **Reyee EG device**, you may use either 192.168.110.1 or 10.44.77.254 to access the device.

For the **Reyee switches**, you may use 10.44.77.200 to access the device.

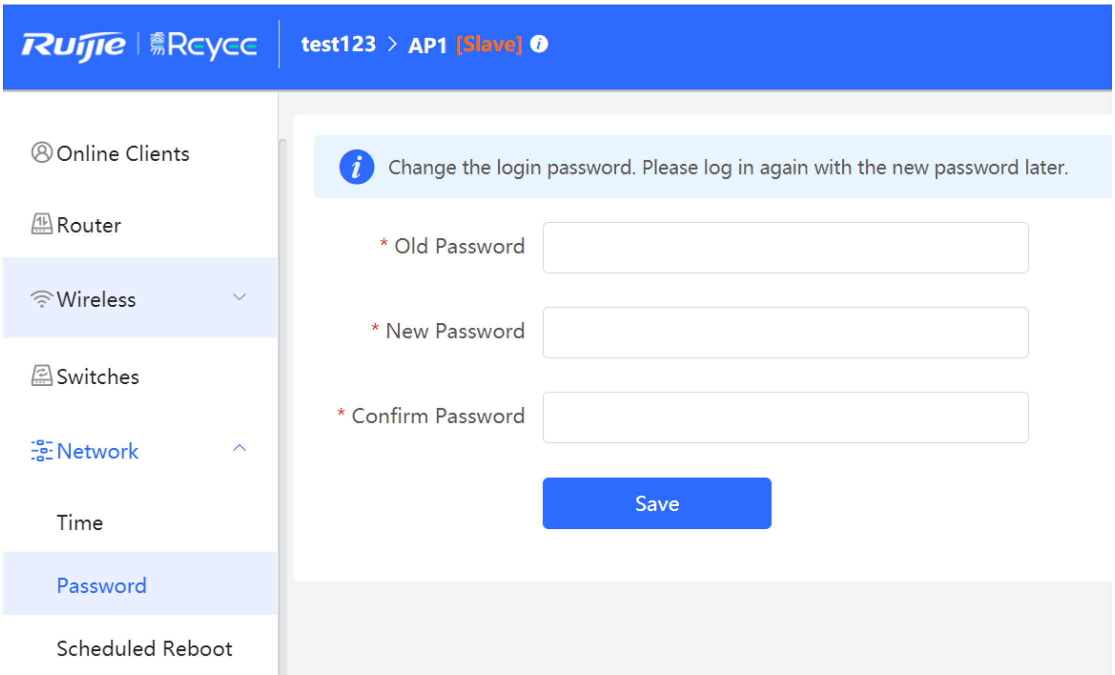
For the **Reyee AP**, you may use either 192.168.120.1 or 10.44.77.254 to access the device.

For the **EST**, you may use 10.44.77.254 to access the device.

The default login password for all Reyee devices is admin.

You may visit https://10.44.77.253 to login to the master device of Reyee network.

2.2 Configuring Password



Change the login password. Please log in again with the new password later.

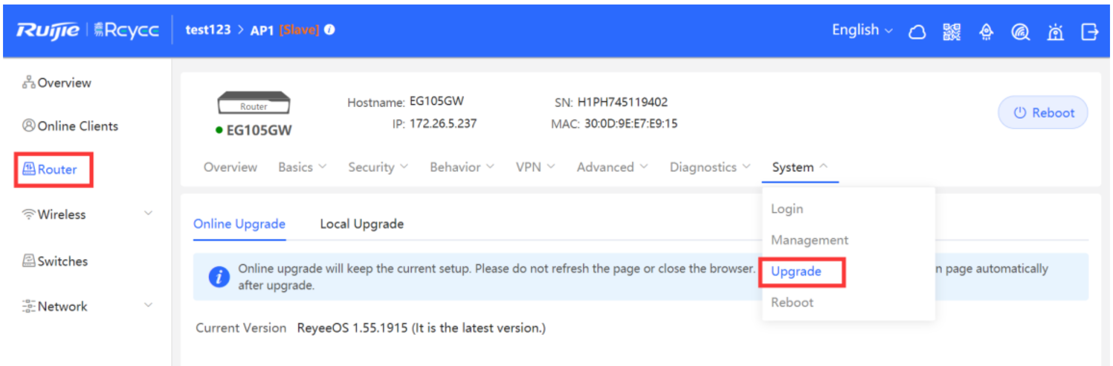
* Old Password

* New Password

* Confirm Password

2.3 Upgrading

Login to the eWeb of the device and choose Router--System--Upgrade.



● EG105GW

Hostname: EG105GW

IP: 172.26.5.237

SN: H1PH745119402

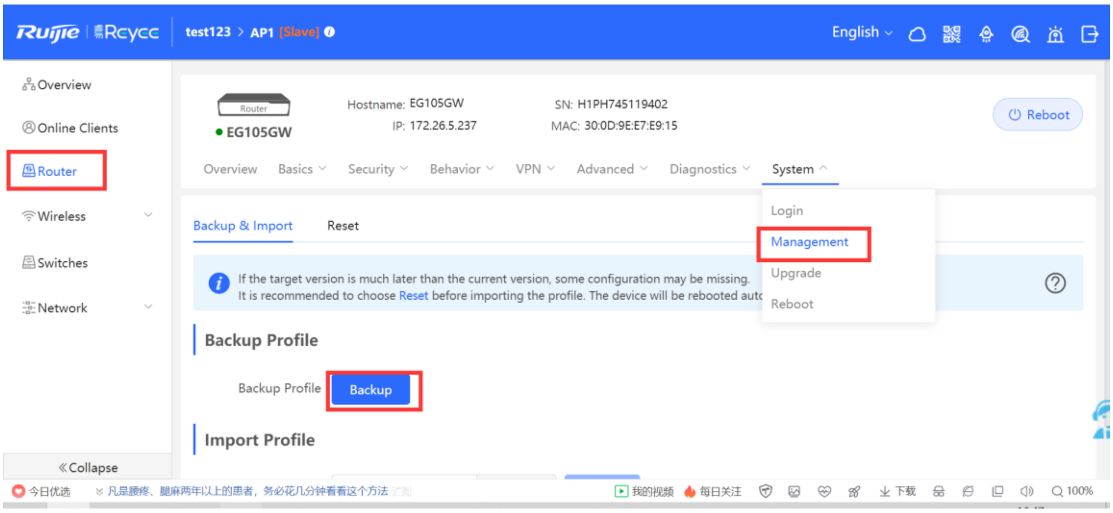
MAC: 30:0D:9E:E7:E9:15

Online upgrade will keep the current setup. Please do not refresh the page or close the browser. n page automatically after upgrade.

Current Version ReyeeOS 1.55.1915 (It is the latest version.)

2.4 Backing up and Resetting

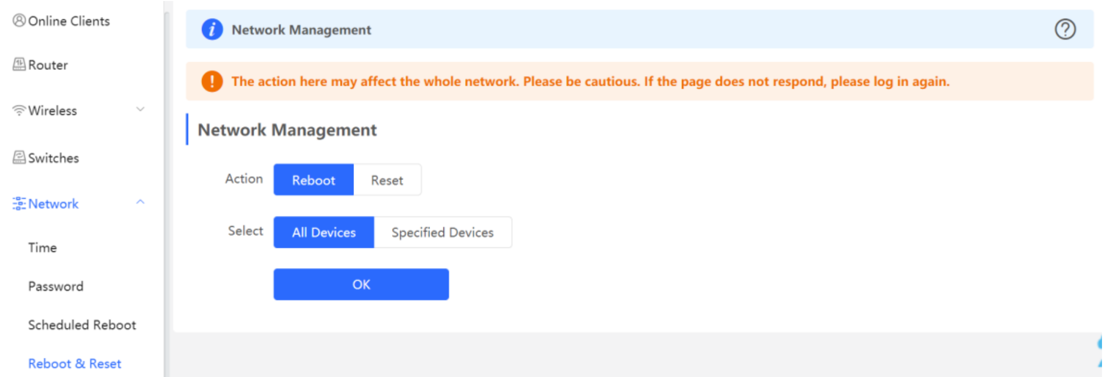
Login in the eWeb of the device and choose Router--System--Management.



Hostname: EG105GW
IP: 172.26.5.237
SN: H1PH745119402
MAC: 30:0D:9E:E7:E9:15

If the target version is much later than the current version, some configuration may be missing.
It is recommended to choose Reset before importing the profile. The device will be rebooted aut

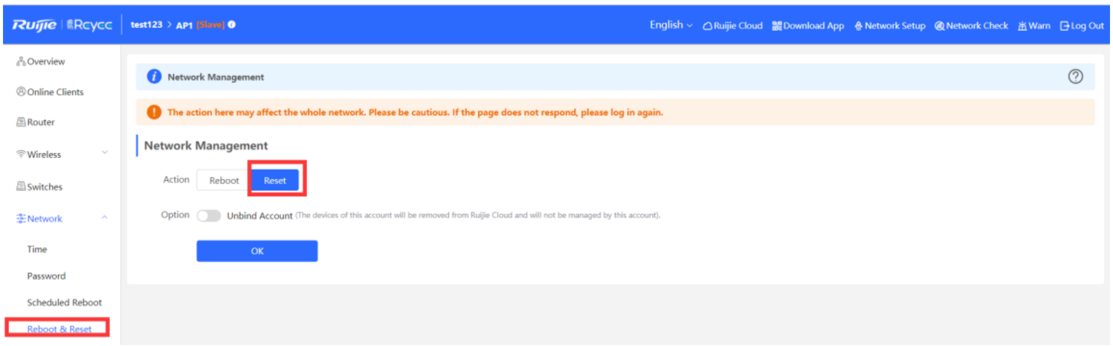
Login in the eWeb of the device and click Network--Reboot&Reset, then you can reset your devices.



The action here may affect the whole network. Please be cautious. If the page does not respond, please log in again.

2.5 Restoring Factory Settings

Login in the eWeb of the device Reset all device in the network.



The action here may affect the whole network. Please be cautious. If the page does not respond, please log in again.

Unbind Account (The devices of this account will be removed from Ruijie Cloud and will not be managed by this account).

3 Getting Start

3.1 Preparing for Installation

3.1.1 Safety Suggestions

To avoid personal injury and equipment damage, please carefully read the safety suggestions before you install each device. The following safety suggestions do not cover all possible dangers

1. 3.1.1.1 Installation

a) Keep the chassis clean and free from any dust.

b) Do not place devices in a walking area.

c) Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance

2. 3.1.1.2 Movement

a) Do not frequently move devices.

b) When moving devices, note the balance and avoid hurting legs and feet or straining the back.

c) Before moving devices, turn off all power supplies and dismantle all power modules.

3. 3.1.1.3 Electricity

a) Observe local regulations and specifications when performing electric operations. Relevant operators must be qualified.

b) Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp/wet ground or floor.

c) Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.

d) Try to avoid maintaining the switch that is powered-on alone.

e) Be sure to make a careful check before you shut down the power supply.

f) Do not place the equipment in a damp location. Do not let any liquid enter the chassis

4. 3.1.1.4 Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following:

a) Proper grounding of grounding screws on the back panel of the device. Use of a three-wire single-phase socket with protective earth wire (PE) as the AC power socket.

b) Indoor dust prevention

c) Proper humidity conditions

5. 3.1.1.5 Laser

Some devices support varying models of optical modules sold on the market which are Class I laser products. Improper use of optical modules may cause damage. Therefore, pay attention to the following when you use them:

a) When a fiber transceiver works, ensure that the port has been connected with an optical fiber or is covered with a dust cap, to keep out dust and avoid burning your eyes.

b) When the optical module is working, do not pull out the fiber cable and stare into the transceiver interface or you may hurt your eyes.

3.1.2 Installation Site Requirement

To ensure the normal working and a prolonged durable life of the equipment, the installation site must meet the following requirements

1. 3.1.2.1 Ventilation

For installing devices, a sufficient space (at least 10 cm distances from both sides and the back plane of the cabinet) should be reserved at the ventilation openings to ensure the normal ventilation. After various cables have been connected, they should be arranged into bundles or placed on the cabling rack to avoid blocking the air inlets. It is recommended to clean the switch at regular intervals (like once every 3 months). Especially, avoid dust from blocking the screen mesh on the back of the cabinet.

2. 3.1.2.2 Temperature and Humidity

To ensure the normal operation and prolong the service life of router, you should keep proper temperature and humidity in the equipment room.

If the equipment room has temperature and humidity that do not meet the requirements for a long time, the equipment may be damaged.

In an environment with relatively high humidity, the insulating material may have bad insulation or even leak electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.

In an environment with relatively low humidity, however, the insulating strip may dry and shrink. Static electricity may occur easily and endanger the circuit on the equipment.

In an environment with high temperature, the equipment is subject to even greater harm, as its performance may degrade significantly and various hardware faults may occur.

3. 3.1.2.3 Cleanness

Dust poses a severe threat to the running of the equipment. The indoor dust falling on the equipment may be adhered by the static electricity, causing bad contact of the metallic joint. Such electrostatic adherence may occur more easily when the relative humidity is low, not only affecting the useful life of the equipment, but also causing communication faults.

4. 3.1.2.4 Grounding

A good grounding system is the basis for the stable and reliable operation of devices. It is the chief condition to prevent lightning stroke and resist interference. Please carefully check the grounding conditions on the installation site according to the grounding requirements, and perform grounding operations properly as required

Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, download conductor and the connector to the grounding system, which usually shares the power reference ground and yellow/green safety cable ground. The lightning discharge ground is for the facility only, irrelevant to the equipment.

EM C Grounding

The grounding required for EMC design includes shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1Ω

5. 3.1.2.5 EMI

Electro-Magnetic Interference (EMI), from either outside or inside the equipment or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component via the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from the electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment and is difficult to shield.

a) For the AC power supply system TN, single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through the filtering circuit.

b) The grounding device of the switch must not be used as the grounding device of the electrical equipment or anti-lightning grounding device. In addition, the grounding device of the switch must be deployed far away from the grounding device of the electrical equipment and anti-lightning grounding device.

c) Keep the equipment away from high-power radio transmitter, radar transmitting station, and high-frequency large-current device.

d) Measures must be taken to shield static electricity.

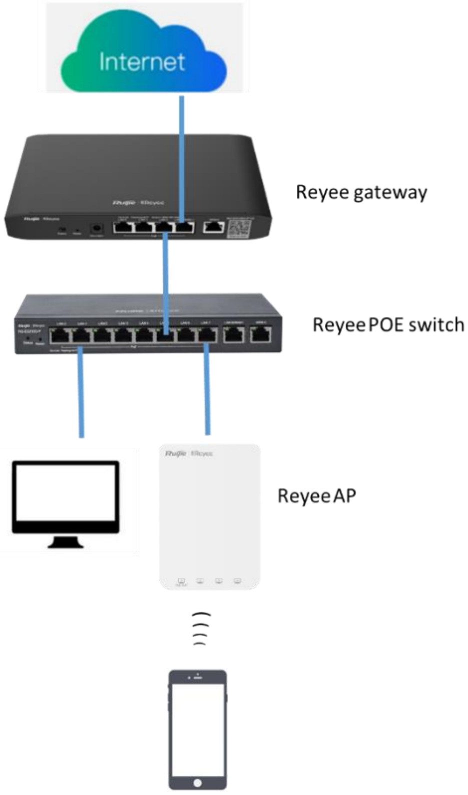
e) Interface cables should be laid inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning

3.1.3 Network Planning

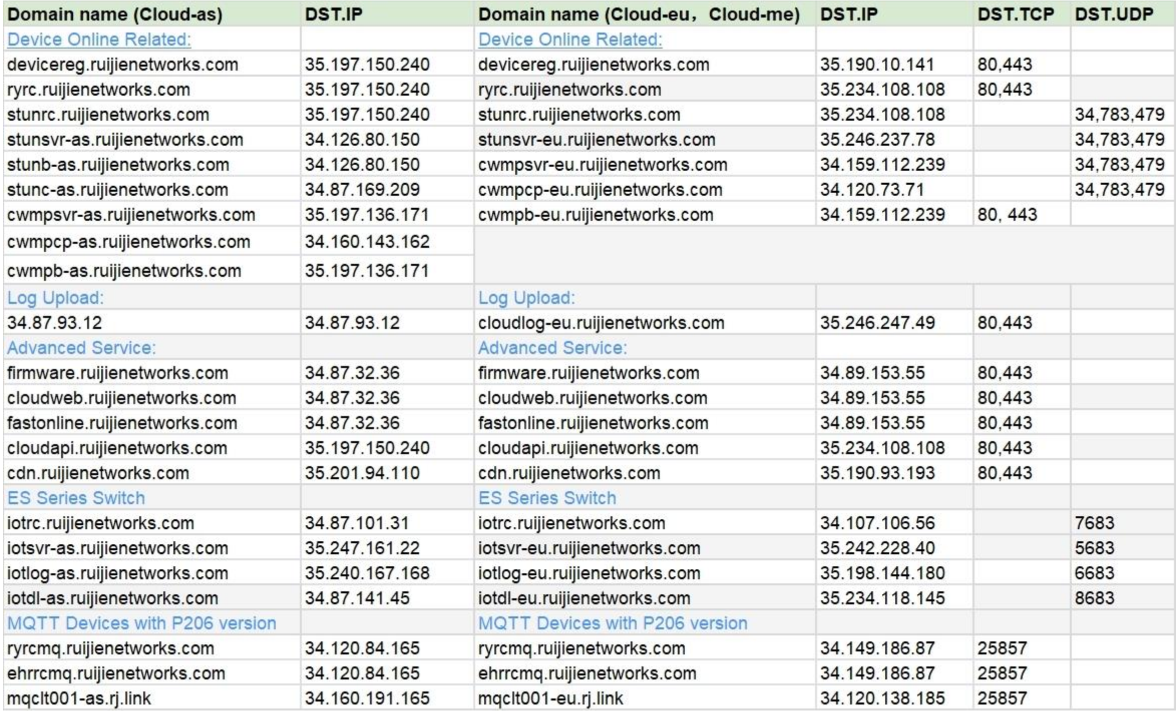
The DHCP server has two address pools on the egress gateway:

192.168.110.0/24 in VLAN 1 for devices of this network

192.168.10.0/24 in VLAN 10 for clients of this network



Following ports are used for Ruijie Cloud management. To let devices go online on Ruijie Cloud, ensure these ports are available and the data stream is permitted in this network.

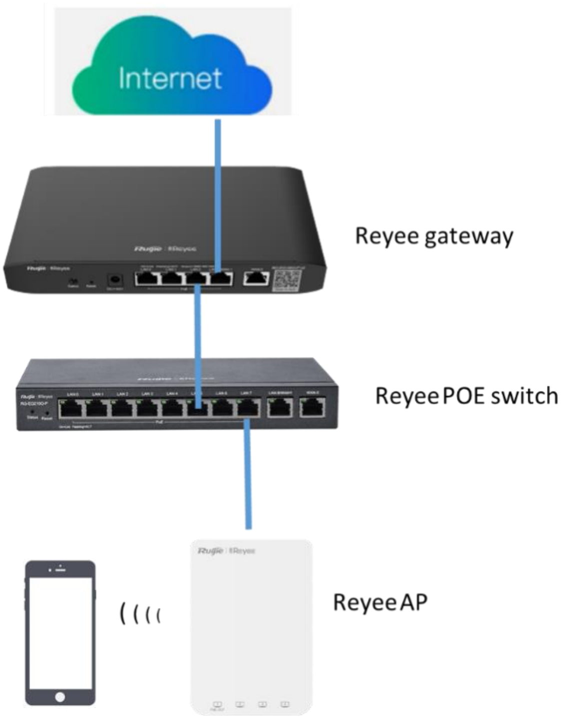


Domain name (Cloud-as)	DST.IP	Domain name (Cloud-eu，Cloud-me)	DST.IP	DST.TCP	DST.UDP
Device Online Related:		Device Online Related:			
devicereg.ruijienetworks.com	35.197.150.240	devicereg.ruijienetworks.com	35.190.10.141	80,443	
ryrc.ruijienetworks.com	35.197.150.240	ryrc.ruijienetworks.com	35.234.108.108	80,443	
stunrc.ruijienetworks.com	35.197.150.240	stunrc.ruijienetworks.com	35.234.108.108		34,783,479
stunsvr-as.ruijienetworks.com	34.126.80.150	stunsvr-eu.ruijienetworks.com	35.246.237.78		34,783,479
stunb-as.ruijienetworks.com	34.126.80.150	cwmpsvr-eu.ruijienetworks.com	34.159.112.239		34,783,479
stunc-as.ruijienetworks.com	34.87.169.209	cwmpcp-eu.ruijienetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.ruijienetworks.com	35.197.136.171	cwmpb-eu.ruijienetworks.com	34.159.112.239	80, 443	
cwmpcp-as.ruijienetworks.com	34.160.143.162				
cwmpb-as.ruijienetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.ruijienetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.ruijienetworks.com	34.87.32.36	firmware.ruijienetworks.com	34.89.153.55	80,443	
cloudweb.ruijienetworks.com	34.87.32.36	cloudweb.ruijienetworks.com	34.89.153.55	80,443	
fastonline.ruijienetworks.com	34.87.32.36	fastonline.ruijienetworks.com	34.89.153.55	80,443	
cloudapi.ruijienetworks.com	35.197.150.240	cloudapi.ruijienetworks.com	35.234.108.108	80,443	
cdn.ruijienetworks.com	35.201.94.110	cdn.ruijienetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.ruijienetworks.com	34.87.101.31	iotrc.ruijienetworks.com	34.107.106.56		7683
iotsvr-as.ruijienetworks.com	35.247.161.22	iotsvr-eu.ruijienetworks.com	35.242.228.40		5683
iotlog-as.ruijienetworks.com	35.240.167.168	iotlog-eu.ruijienetworks.com	35.198.144.180		6683
iotdl-as.ruijienetworks.com	34.87.141.45	iotdl-eu.ruijienetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.ruijienetworks.com	34.120.84.165	ryrcmq.ruijienetworks.com	34.149.186.87	25857	
ehrrcmq.ruijienetworks.com	34.120.84.165	ehrrcmq.ruijienetworks.com	34.149.186.87	25857	
mqclt001-as.rj.link	34.160.191.165	mqclt001-eu.rj.link	34.120.138.185	25857	

3.2 Quick Provisioning

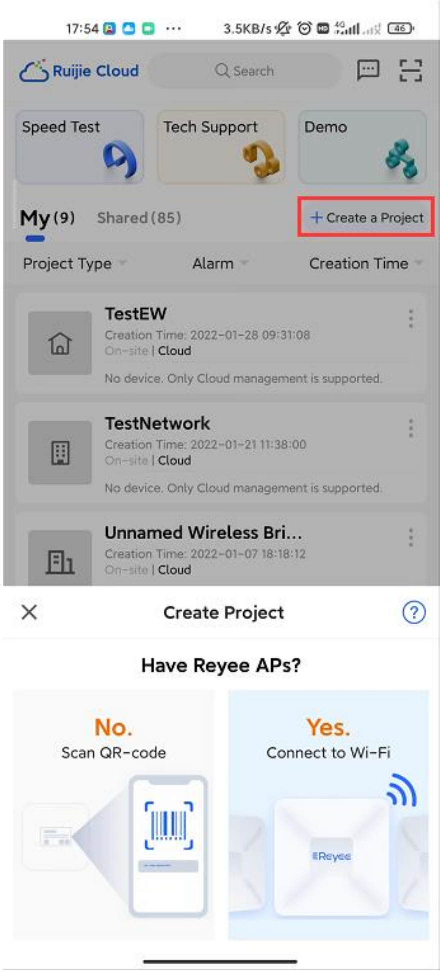
3.2.1 Quick provisioning via Ruijie Cloud APP

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.



1. **3.2.1.1 Create a project**

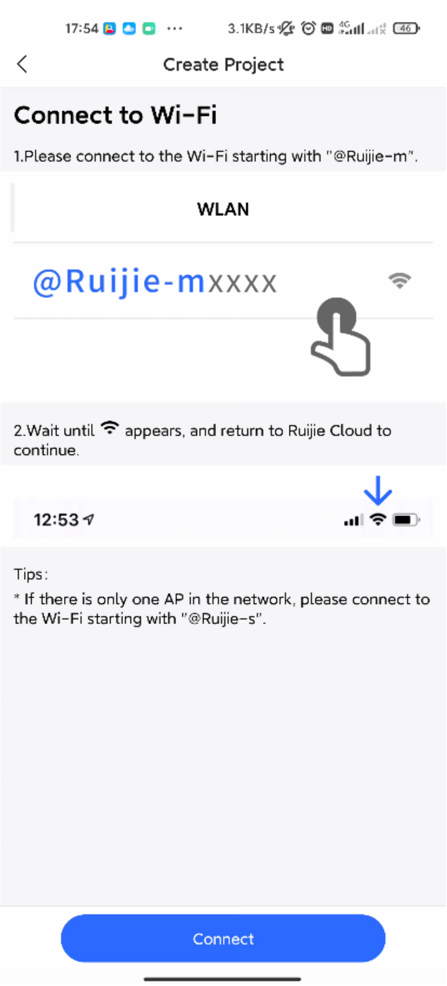
Open Ruijie Cloud App and Click **Create a Project,** then select **Connect to Wi-Fi.**



After click **Yes**, then Cloud App will prompt you to connect @Ruijie-mxxxx SSID.

Note:

@Ruijie-mxxxx is generated after network self-organization established successfully, while @Ruijie-sxxxx is generated on a standalone device, xxxx is the last four letters of mac address of device.



17:54 ··· 3.1KB/s

Create Project

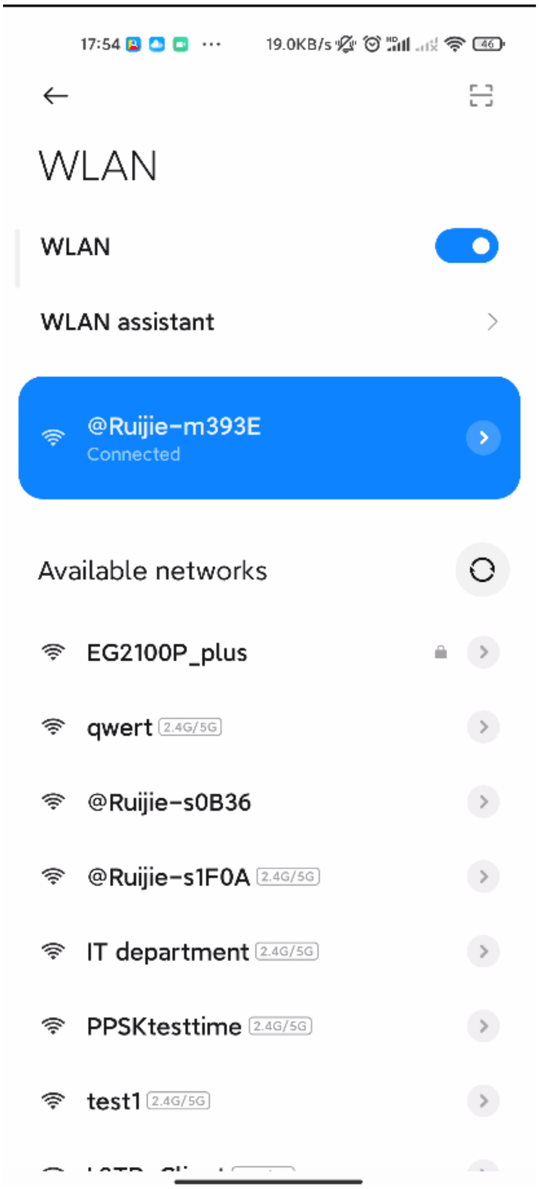
Connect to Wi-Fi

1.Please connect to the Wi-Fi starting with "@Ruijie-m".

2.Wait until ᯤ appears, and return to Ruijie Cloud to continue.

Tips:
* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".

Connect the @Ruijie-mxxxx SSID on your phone.



WLAN

WLAN

WLAN assistant

@Ruijie-m393E
Connected

Available networks

EG2100P_plus

qwert 2.4G/5G

@Ruijie-s0B36

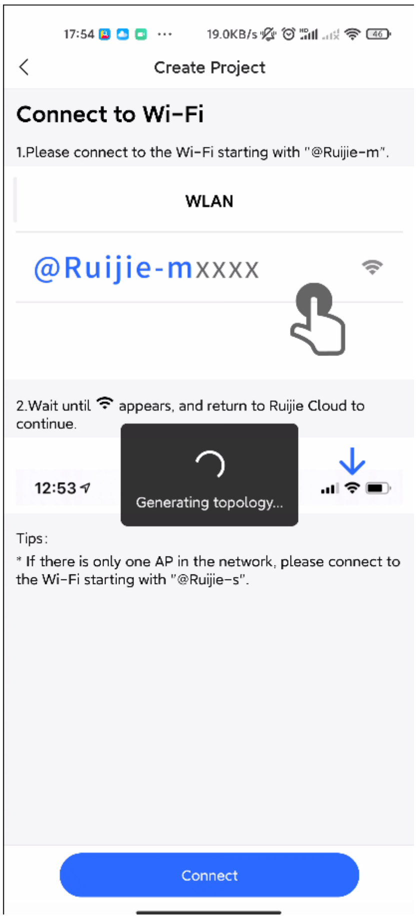
@Ruijie-s1F0A 2.4G/5G

IT department 2.4G/5G

PPSKtesttime 2.4G/5G

test1 2.4G/5G

After connected the @Ruijie-mxxxx SSID, the Cloud App will prompt to generate topology and detect all devices in this SON.



Create Project

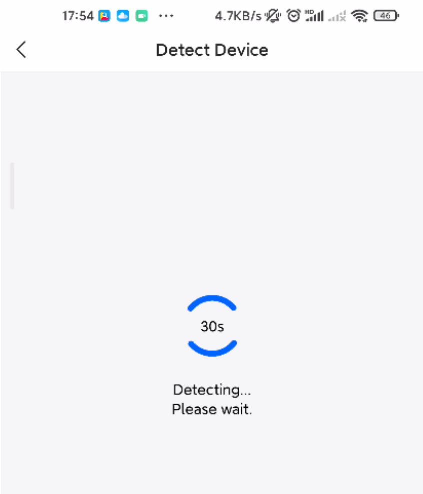
Connect to Wi-Fi

1.Please connect to the Wi-Fi starting with "@Ruijie-m".

2.Wait until appears, and return to Ruijie Cloud to continue.

Tips:

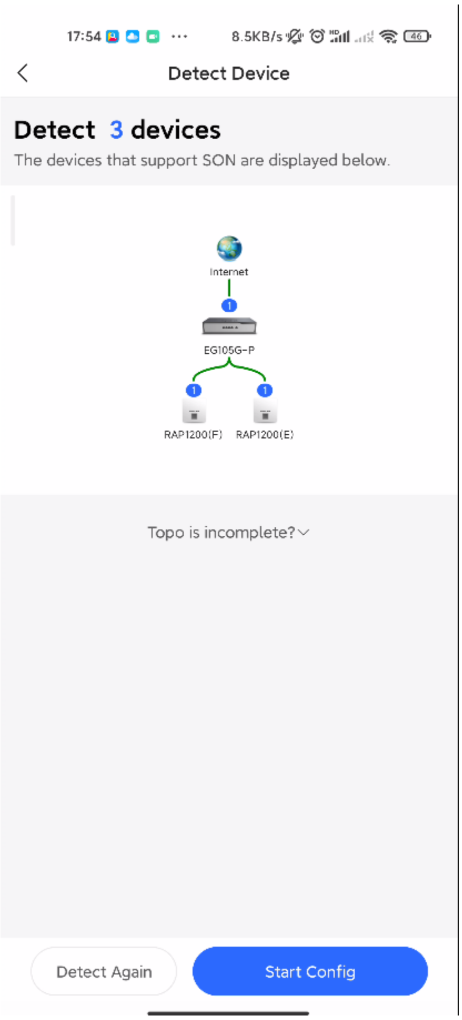
* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".



Detect Device

Detecting...
Please wait.

After all devices were detected, Cloud App will display them and show the topology, shown in the below picture. Click **Start Config** to perform the basic configuration of this project.



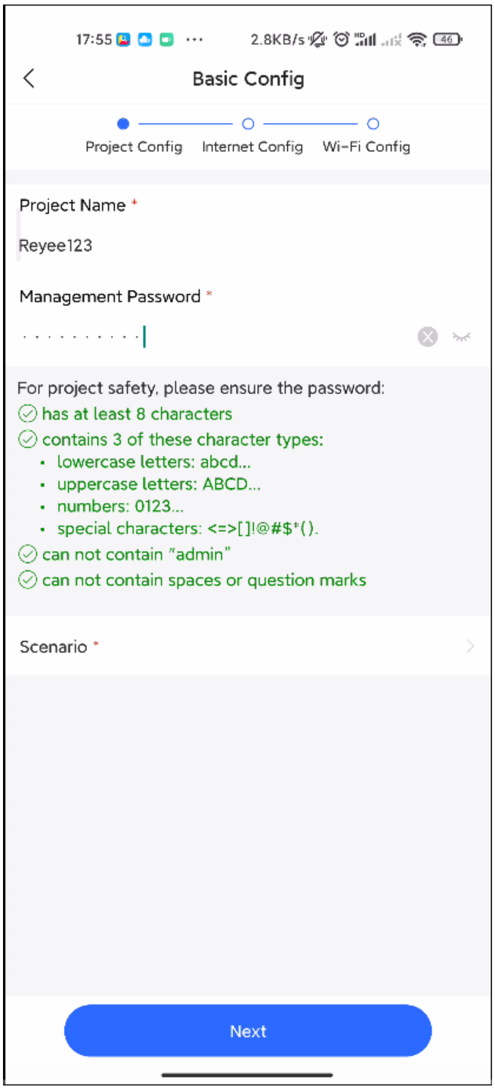
Detect Device

Detect 3 devices

The devices that support SON are displayed below.

2. 3.2.1.2 Configure the project

Input the Project Name and Management Password.



Project Name *

Reyee123

Management Password *

··········

For project safety, please ensure the password:

✓ has at least 8 characters

✓ contains 3 of these character types:

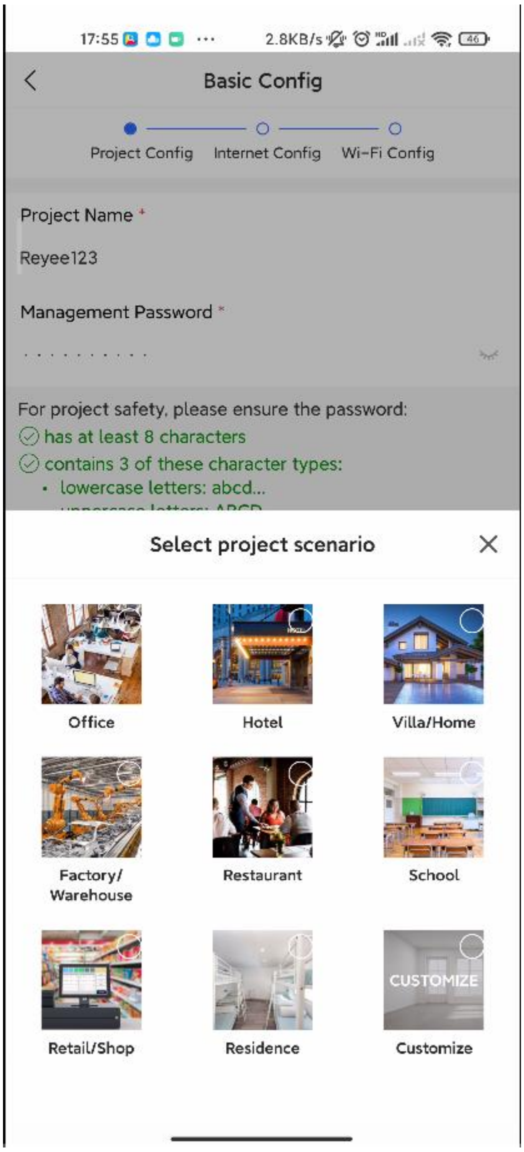
- lowercase letters: abcd...
- uppercase letters: ABCD...
- numbers: 0123...
- special characters: <=>[]!@#$*().

✓ can not contain "admin"

✓ can not contain spaces or question marks

Scenario *

Then select the scenario of this project based on your requirement.



Basic Config

● Project Config ○ Internet Config ○ Wi-Fi Config

Project Name *

Reyee123

Management Password *

· · · · · · · · · ·

For project safety, please ensure the password:

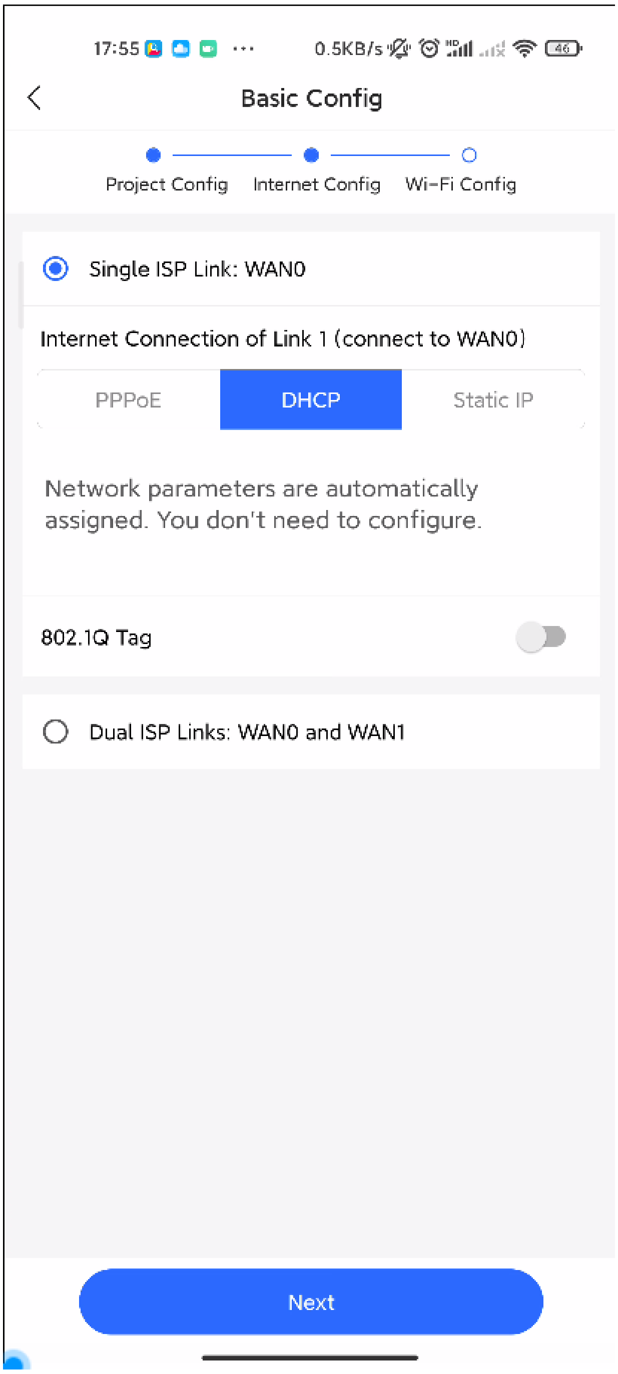
✓ has at least 8 characters

✓ contains 3 of these character types:

- lowercase letters: abcd...

3. 3.2.1.3 Configure the internet

For configuring WAN, you can chose PPPoE, DHCP and Static IP.



Basic Config

● Project Config ● Internet Config ○ Wi-Fi Config

● Single ISP Link: WAN0

Internet Connection of Link 1 (connect to WAN0)

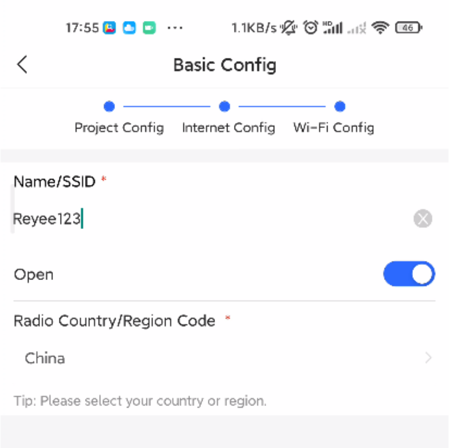
Network parameters are automatically assigned. You don't need to configure.

802.1Q Tag

○ Dual ISP Links: WAN0 and WAN1

4. 3.2.1.4 Configure the SSID

For SSID settings, input the name of SSID and configure it as open or configure password for this SSID. Select the region code.


17:55 ··· 1.1KB/s

Basic Config

Project Config · Internet Config · Wi-Fi Config

Name/SSID *

Reyee123

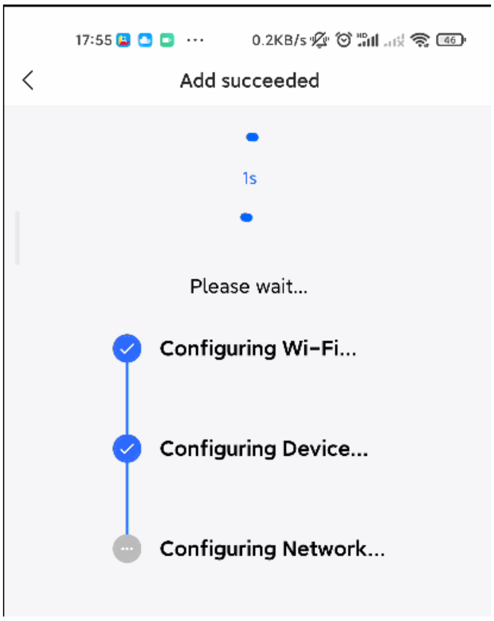
Open ●

Radio Country/Region Code *

China

Tip: Please select your country or region.

The configuration will be synchronized to the network


17:55 ··· 0.2KB/s

Add succeeded

1s

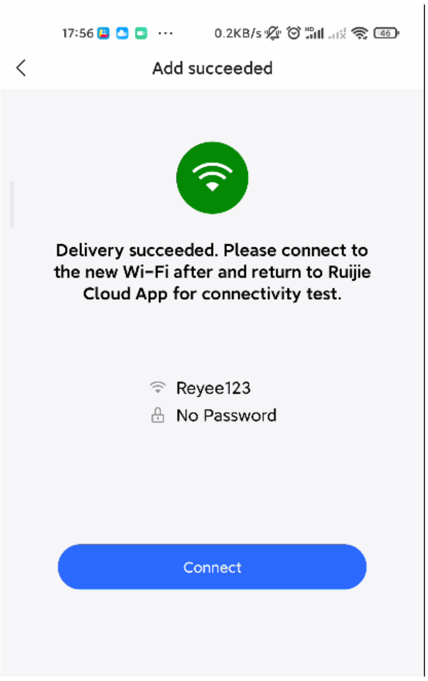
Please wait...

✓ Configuring Wi-Fi...

✓ Configuring Device...

··· Configuring Network...

After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.


17:56 ··· 0.2KB/s

Add succeeded

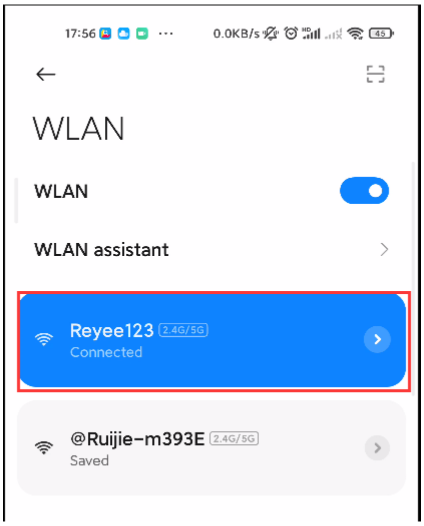
Delivery succeeded. Please connect to the new Wi-Fi after and return to Ruijie Cloud App for connectivity test.

Reyee123

No Password

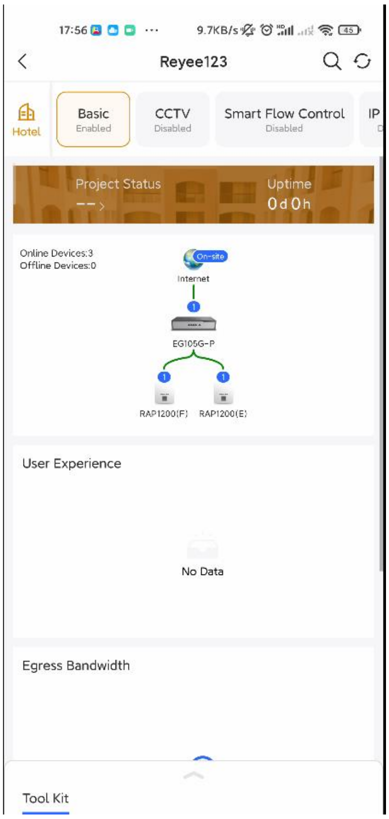
Connect

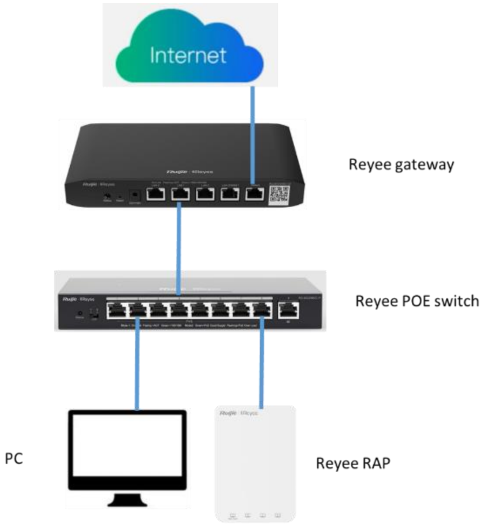
Connect to the SSID created just now to manage the whole network on Cloud App.



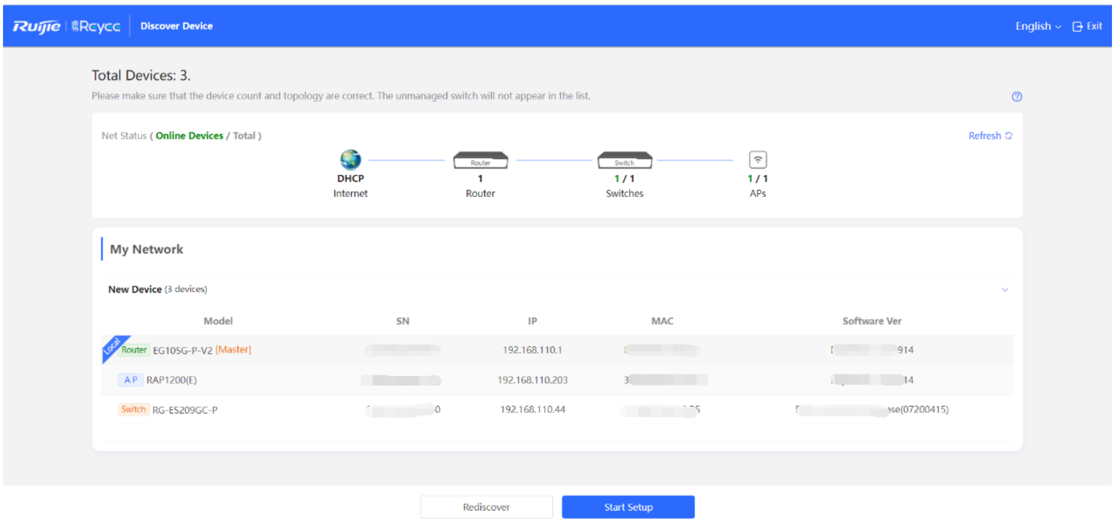
3.2.2 Quick provisioning via Reyee EWeb

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.





Connect PC to POE switch, set the ip address of PC as static ip address 192.168.110.x, then input 192.168.110.1 on the browser to login the EWEB of EG. All devices in this networks will display in EWEB. Click the Start Setup to perform the quick start of this network.



Total Devices: 3.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

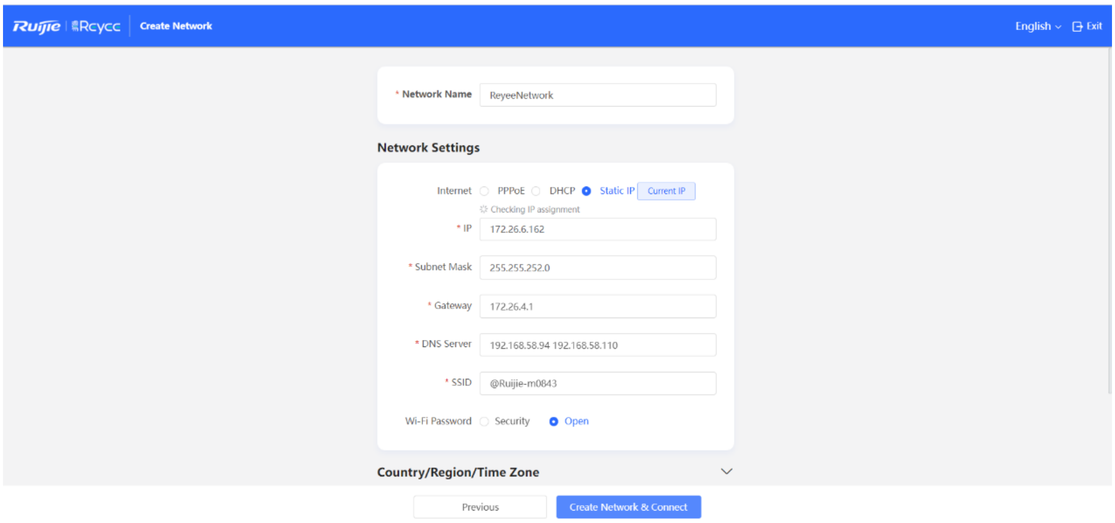
Net Status (Online Devices / Total)

My Network

New Device (3 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105G-P-V2 [Master]	[redacted]	192.168.110.1	[redacted]	[redacted]914
AP RAP1200(E)	[redacted]	192.168.110.203	3[redacted]	[redacted]14
Switch RG-ES209GC-P	[redacted]0	192.168.110.44	[redacted]5	[redacted]se(07200415)

Show in the below picture, to finish the quick start of this network, you need to input the network name, configure the manner to access internet of this network and input the password of SSID or set the SSID as open. After select the Country/Region and click **Create Network & Connect,** the configuration will be delivery and activated, shown as the below two picture.



Create Network

English Exit

* Network Name: ReyeeNetwork

Network Settings

Internet: ○ PPPoE ○ DHCP ● Static IP Current IP

Checking IP assignment

* IP: 172.26.6.162

* Subnet Mask: 255.255.252.0

* Gateway: 172.26.4.1

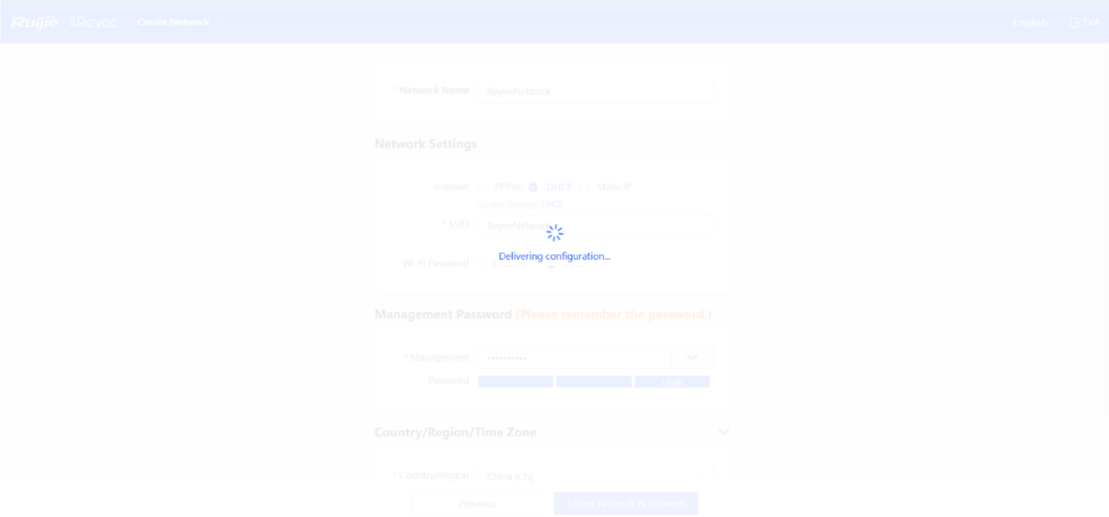
* DNS Server: 192.168.58.94 192.168.58.110

* SSID: @Ruijie-m0843

Wi-Fi Password: ○ Security ● Open

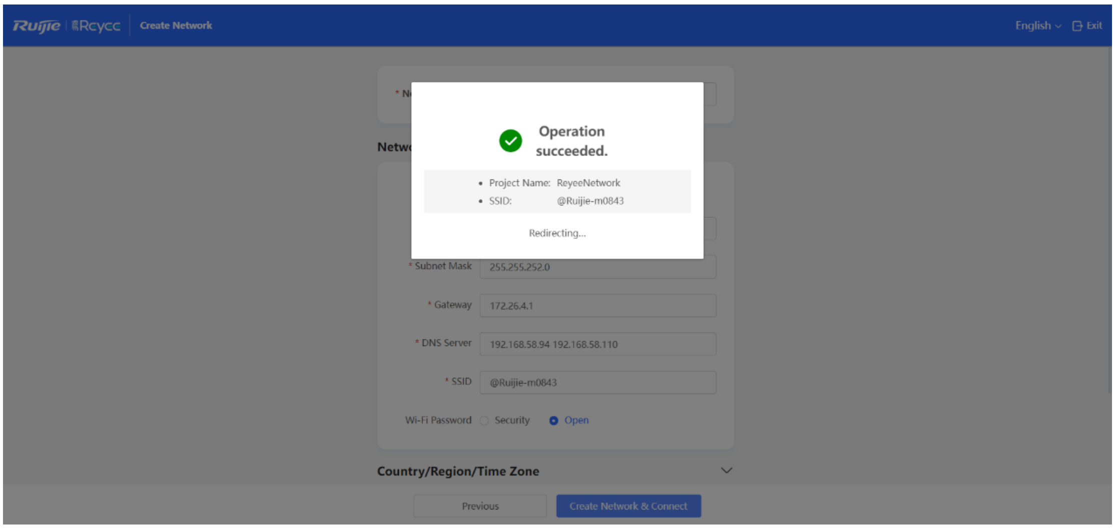
Country/Region/Time Zone

Previous | Create Network & Connect



Delivering configuration...

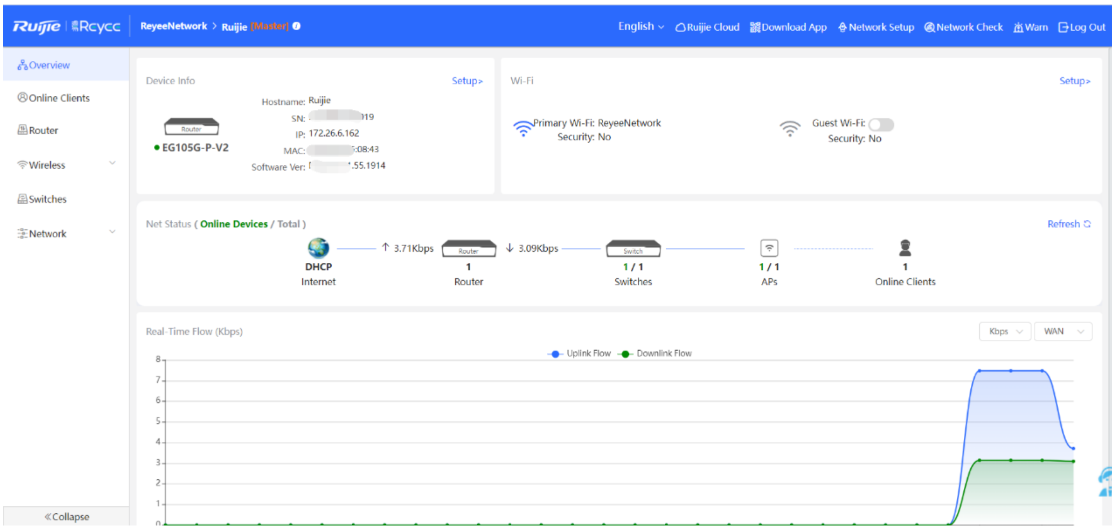
After the configuration has been delivery and activated, you can enter the overview interface to manage the SON of Reyee devices.



Operation succeeded.

- Project Name: ReyeeNetwork
- SSID: @Ruijie-m0843

Redirecting...



● EG105G-P-V2

Hostname: Ruijie
SN: [redacted]19
IP: 172.26.6.162
MAC: [redacted]:08:43
Software Ver: [redacted].55.1914

Primary Wi-Fi: ReyeeNetwork
Security: No

Guest Wi-Fi: ○
Security: No

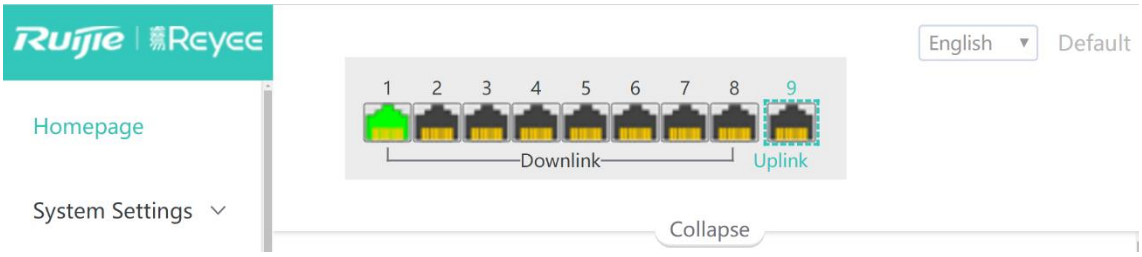
DHCP Internet — ↑ 3.71Kbps — 1 Router — ↓ 3.09Kbps — 1 / 1 Switches — 1 / 1 APs — 1 Online Clients

4 ES Series Switches Port Settings

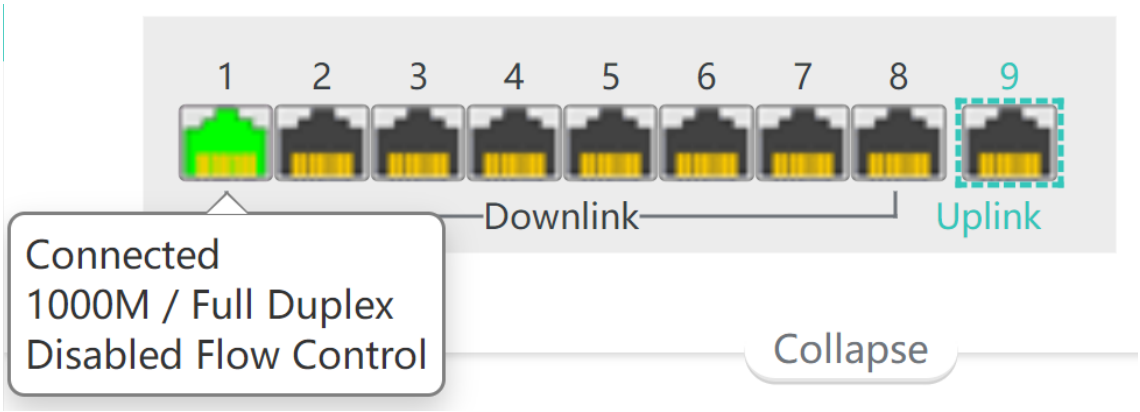
4.1 Managing Port Information

4.1.1 Port Status Bar

The port status bar is at the top of the web page, showing port ID, port attribute (uplink/downlink), and the connection status. Click **Collapse** to hide the port status bar.

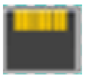
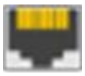
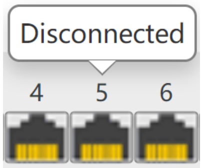
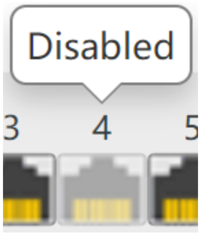
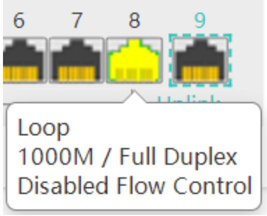
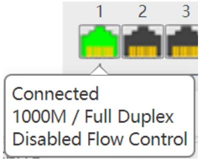
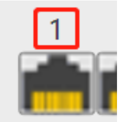
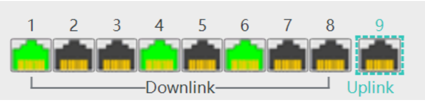


Different colors and shapes of the port icons represent different port statuses. See Table 2-1 for details. Move the cursor over a port icon and the port status will be displayed, including the connection status, port rate, duplex mode, and flow control status.



Connected
1000M / Full Duplex
Disabled Flow Control

Table 4-1 Port Icons

Port Icon	Description
	The port icon is in the shape of a square, showing the port is a fiber port.
	The port icon is in the shape of an RJ-45 connector, showing the port is a copper port.
	The color of the port icon is black, showing the port is disconnected.
	The color of the port icon is gray, showing the port is disabled and cannot receive or transmit packets.
 6 7 8 9 Loop 1000M / Full Duplex Disabled Flow Control	The color of the port icon is yellow, showing there is a loop.
 1 2 3 Connected 1000M / Full Duplex Disabled Flow Control	The color of the port icon is green, showing the port is working normally.
	The number above the port icon is the port ID used to identify the device port. With the port ID, users can specify the port they want to configure.
 1 2 3 4 5 6 7 8 9 Downlink Uplink	The device port is classified into the uplink port and the downlink port. The uplink port is used to connect network devices in the upper layer and access the core network. The downlink port is used to connect the endpoints. When port isolation is enabled, the downlink ports of the device are isolated from each other, and they can only communicate with the uplink ports. For details, see Chapter 2.4.

4.1.2 Port Info Overview

Choose **Homepage**.

The homepage displays the global port information, including the port status, the packet receiving/transmission rate (Rx/Tx rate), port isolation status and loop detection status. Besides, it supports searching for the downlink device.

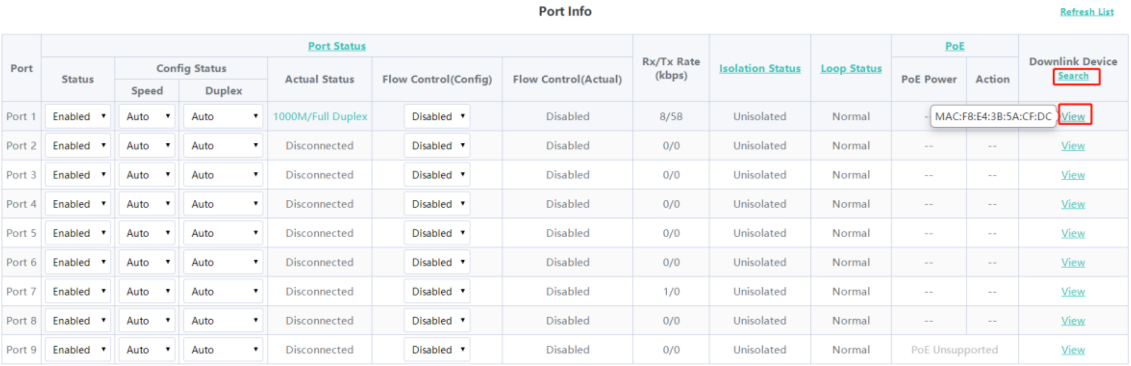
Click **Port Status** to configure the basic port attributes. For details, see Chapter 2.2.

Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see Chapter 2.4.

Click **Loop Status** to enable loop guard function. After a loop occurs, the port causing the loop will be shut down automatically. For details, see 4.3.

Click **Search** in the **Downlink Device** column to search for the downlink device of the selected port. After the search is done, click **View** to view the MAC address of the downlink device.

Click **Refresh List** to fetch the latest port information.



Port Info

Refresh List

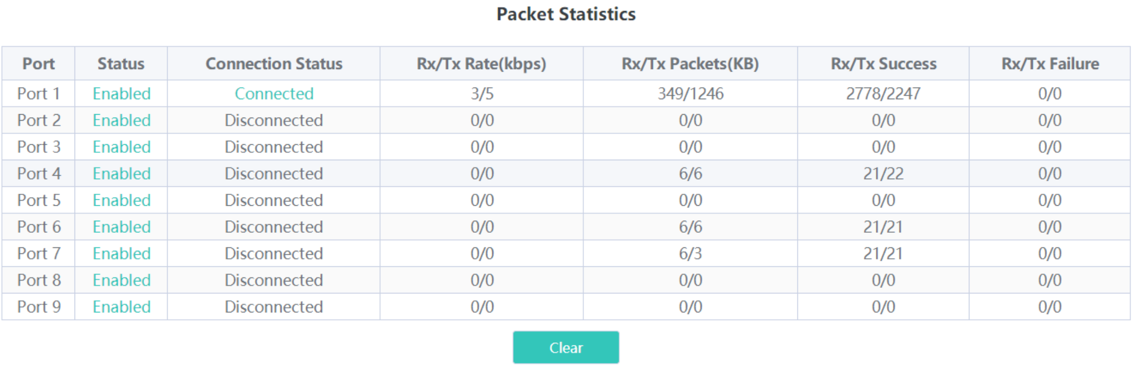
Port	Port Status						Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device Search
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)				PoE Power	Action	
		Speed	Duplex									
Port 1	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	8/58	Unisolated	Normal	-	MAC:F8:E4:3B:5A:CF:DC	View
Port 2	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 4	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 6	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 7	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	1/0	Unisolated	Normal	--	--	View
Port 8	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	--	--	View
Port 9	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	0/0	Unisolated	Normal	PoE Unsupported		View

4.1.3 Port Packet Statistics

Choose **Monitoring** > **Packet Statistics**.

The **Packet Statistics** page displays the port status, the connection status, Rx/Tx rate (kbps), Rx/Tx packets (KB), Rx/Tx success, and Rx/Tx failure.

Click **Clear** to clear current packet statistics of all ports and reset the statistics.



Packet Statistics

Port	Status	Connection Status	Rx/Tx Rate(kbps)	Rx/Tx Packets(KB)	Rx/Tx Success	Rx/Tx Failure
Port 1	Enabled	Connected	3/5	349/1246	2778/2247	0/0
Port 2	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 3	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 4	Enabled	Disconnected	0/0	6/6	21/22	0/0
Port 5	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 6	Enabled	Disconnected	0/0	6/6	21/21	0/0
Port 7	Enabled	Disconnected	0/0	6/3	21/21	0/0
Port 8	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 9	Enabled	Disconnected	0/0	0/0	0/0	0/0

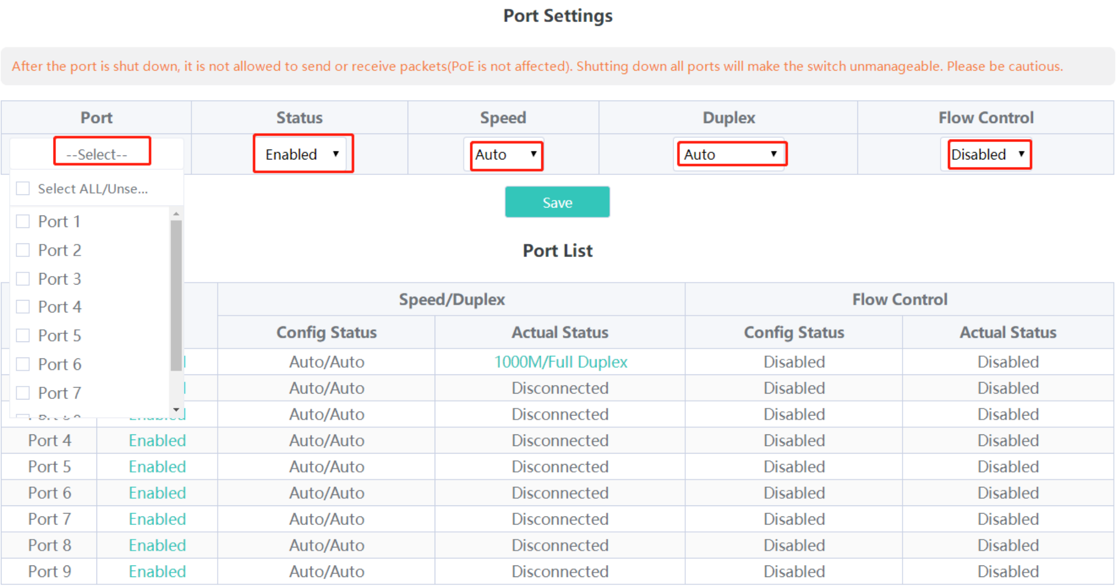
4.2 Setting and Viewing Port Attributes

Choose **Switch Settings** > **Port Settings**.

4.2.1 Port Settings

Users can set the basic attributes of the Ethernet ports in batches.

Click **Select** in the **Port** column to display options of all device ports. Select the ports you want to configure, and then select the port status, port rate, port duplex mode, flow control status, and click **Save**.



Port Settings

After the port is shut down, it is not allowed to send or receive packets(PoE is not affected). Shutting down all ports will make the switch unmanageable. Please be cautious.

Port	Status	Speed	Duplex	Flow Control
--Select--	Enabled ▾	Auto ▾	Auto ▾	Disabled ▾

□ Select ALL/Unse...
□ Port 1
□ Port 2
□ Port 3
□ Port 4
□ Port 5
□ Port 6
□ Port 7

Port List

		Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
		Auto/Auto	1000M/Full Duplex	Disabled	Disabled
		Auto/Auto	Disconnected	Disabled	Disabled
		Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

Table 4-2 Basic Port Configuration Parameters

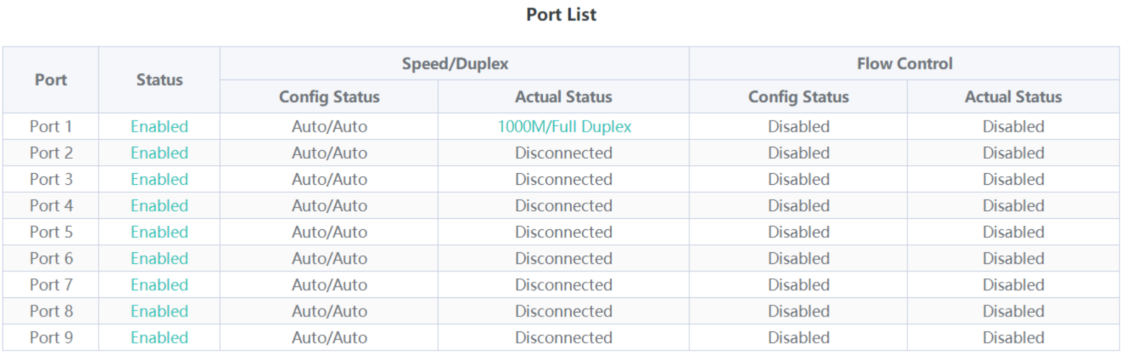
Parameter	Description	Default
Port	Select the ports you want to configure.	NA
Status	When the port is disabled, it cannot receive or transmit packets (PoE is not affected).	Enabled
Speed	Configure the operating speed of the Ethernet physical port. When the speed is set to **Auto**, it means that it is determined by the auto-negotiation between the local port and the peer port. The negotiated speed can be any speed within the port capability.	Auto
Duplex	● Full duplex: The port can receive packets while sending packets. ● Half duplex: The port can receive or send packets at a time. ● Auto-negotiation: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port.	Auto
Flow Control	After enabling the flow control feature, the port will process the received flow control frames and send flow control frames when flow congestion occurs.	Disabled

Caution

Shutting down all ports will make the switch unmanageable. Exercise caution when performing this operation.

4.2.2 Port Status

Users can view the configuration status of the port attributes and check whether these configurations are active, including the port rate, duplex mode, and flow control status.



Port List

Port	Status	Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
Port 1	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 2	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 3	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

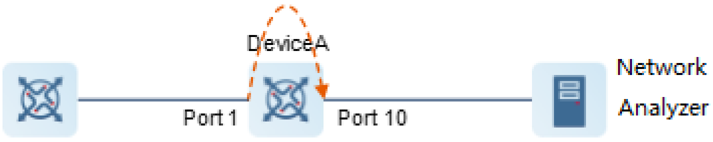
4.3 Port Mirroring

4.3.1 Overview

In network monitoring and troubleshooting scenarios, users need to analyze data traffic on suspicious network nodes or device ports. When port mirroring is enabled, packets received and transmitted on the source port will be mirrored to the mirror port (destination port). Users can monitor and analyze the packets on the mirror port through network analyzer without affecting the normal data forwarding of the monitored device.

As Figure 2-1 shows, by configuring port mirroring on Device A, the packets on Port 1 are mirrored to Port 10. Though the network analyzer is not directly connected to Port 1, it can receive all packets on Port 1 and is able to monitor the data traffic on Port 1.

Figure 4-1 Operating Principle of Port Mirroring



4.3.2 Configuration Steps

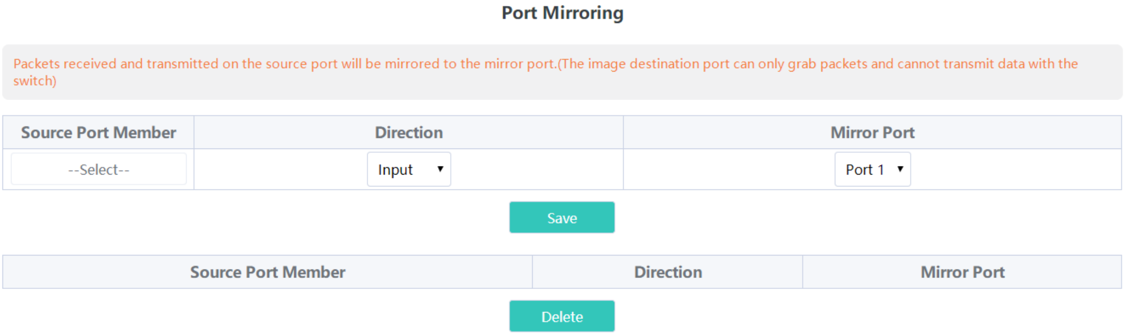
Choose **Switch Settings** > **Port Mirroring**.

Select the source port, the monitoring direction, and the mirror port, and click **Save**. The device supports configuring one port mirroring rule.

If you want to delete port mirroring configuration, click **Delete**.

⚠ **Caution**

- You can select multiple source ports but only one mirror port. The source ports cannot contain the mirror port.
- For RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, RG-ES209GC-P switches, the mirror port only supports packet capture and cannot transmit data with switches.



Port Mirroring

Packets received and transmitted on the source port will be mirrored to the mirror port.(The image destination port can only grab packets and cannot transmit data with the switch)

Source Port Member	Direction	Mirror Port
--Select--	Input	Port 1

Source Port Member	Direction	Mirror Port

Table 4-3 Port Mirroring Parameters

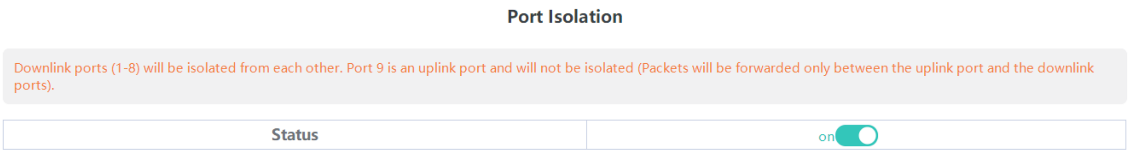
Parameter	Description
Source Port Member	The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. Users can select multiple source ports. Packets on these ports will be mirrored to one mirror port.
Direction	Direction of the data traffic monitored on the source port: ● Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. ● Input: The packets received by the source port will be mirrored to the mirror port. ● Output: The packets transmitted from the sourced port will be mirrored to the mirror port.
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and it transmits packets on the source port to the monitoring device.

4.4 Port Isolation

Choose **Switch Settings** > **Port Isolation**.

Port isolation is used for isolating layer-2 packets. When port isolation is enabled, the downlink ports are isolated from each other but can communicate with uplink ports.

Port isolation is disabled by default. Toggle the switch to **On** to enable port isolation.



Port Isolation

Downlink ports (1-8) will be isolated from each other. Port 9 is an uplink port and will not be isolated (Packets will be forwarded only between the uplink port and the downlink ports).

Status	on

Caution

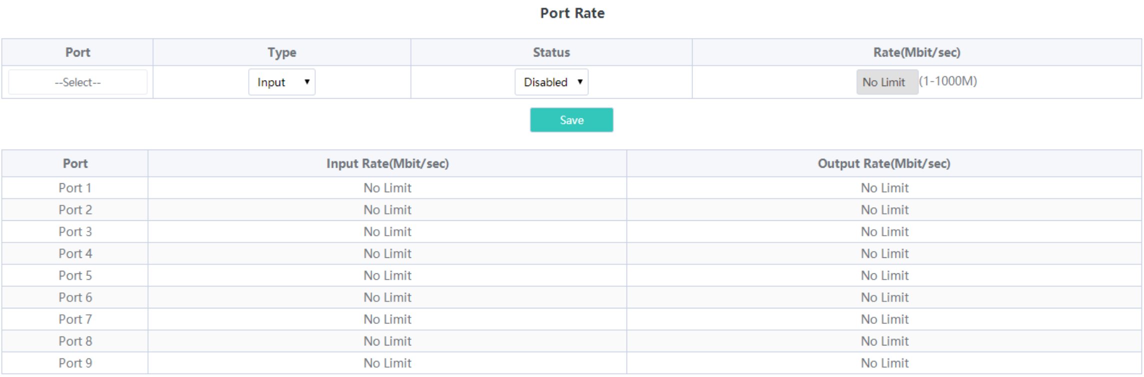
The number of the uplink/downlink ports and port IDs of different devices vary. Please refer to the actual information of the device.

4.5 Port-based Rate Limiting

Choose **QoS Settings** > **Port Rate**.

Users can configure rate limiting rules for packets in the input direction and the output direction of ports. There is no rate limiting on ports by default.

Select the port you want to configure, then select the rate limiting type and status, and enter the rate limit. Click **Save** to save the configuration. The configuration will be displayed accordingly in the **Port Rate** table right below the **Save** button.



Port Rate

Port	Type	Status	Rate(Mbit/sec)
--Select--	Input	Disabled	No Limit (1-1000M)

Port	Input Rate(Mbit/sec)	Output Rate(Mbit/sec)
Port 1	No Limit	No Limit
Port 2	No Limit	No Limit
Port 3	No Limit	No Limit
Port 4	No Limit	No Limit
Port 5	No Limit	No Limit
Port 6	No Limit	No Limit
Port 7	No Limit	No Limit
Port 8	No Limit	No Limit
Port 9	No Limit	No Limit

Table 4-4 Rate Limiting Parameters

Parameter	Description	Default
Port	Users can select multiple ports for rate limiting configuration in batches.	NA
Type	The direction of the rate-limited data traffic: ● Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets. ● Input: Rate limiting for packets received by the port. ● Output: Rate limiting for packets transmitted from the port.	NA
Status	Users can decide whether to enable or disable rate limiting.	Disabled
Rate (Mbit/sec)	The maximum rate at which packets are forwarded over the port.	No limit

Note

- The rate limiting range for RG-ES205C-P switch ports is from 1 to 100M.
- The maximum rate supported by port 1 to port 8 of RG-ES209C-P switch is 100M. If the configured rate exceeds 100M, the effective rate will still be 100M. The rate limiting range for port 9 is from 1 to 1000M.
- The rate limiting range for RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P, RG-FS306-D switches ports is from 1 to 1000M.

4.6 Management IP Address

Choose **System Settings** > **IP Settings**.

Users can configure the management IP address of the device. By accessing the management IP address, users can configure and manage the device.

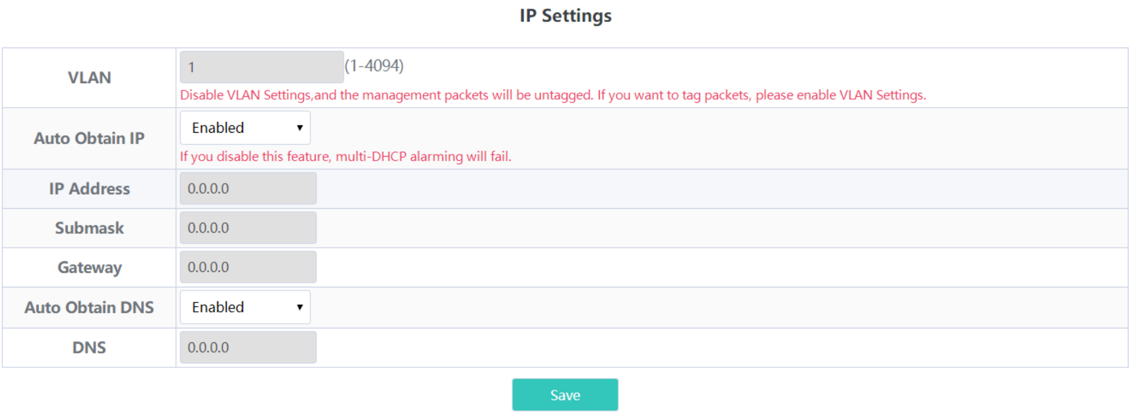
There are two Internet types available:

- Dynamic IP address: Enable **Auto Obtain IP** feature to use the IP address assigned dynamically by the uplink DHCP server.
- Static IP address: Disable **Auto Obtain IP** feature to use the fixed IP address configured manually by the user.

Enable **Auto Obtain IP** feature, and the device will automatically obtain various parameters from the DHCP server. Users can select whether to obtain a DNS address automatically from the DHCP server. If **Auto Obtain DNS** feature is disabled, users need to configure a DNS address manually.

After disabling **Auto Obtain IP** feature, users need to manually configure the IP address, subnet mask, gateway IP address, and DNS address. Click **Save** to enforce the configuration.

VLAN is used for managing VLAN tag of the management packets. Disable VLAN settings, and the management packets will be untagged, and management VLAN configuration is not supported. The management VLAN of the device is VLAN 1 by default.



IP Settings

VLAN	1 (1-4094) Disable VLAN Settings,and the management packets will be untagged. If you want to tag packets, please enable VLAN Settings.
Auto Obtain IP	Enabled ▾ If you disable this feature, multi-DHCP alarming will fail.
IP Address	0.0.0.0
Submask	0.0.0.0
Gateway	0.0.0.0
Auto Obtain DNS	Enabled ▾
DNS	0.0.0.0

Note

- Disable VLAN settings, and the management packets will be untagged. If you want to tag packets, please enable VLAN settings. For details, see Chapter 3.2.1.
- The management VLAN must be selected from the existing VLANs. To create a static VLAN, refer to Chapter 3.2.2.

- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web management system. For details, see Chapter 3.2.3.
- If you disable **Auto Obtain IP** feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see Chapter 7.2.

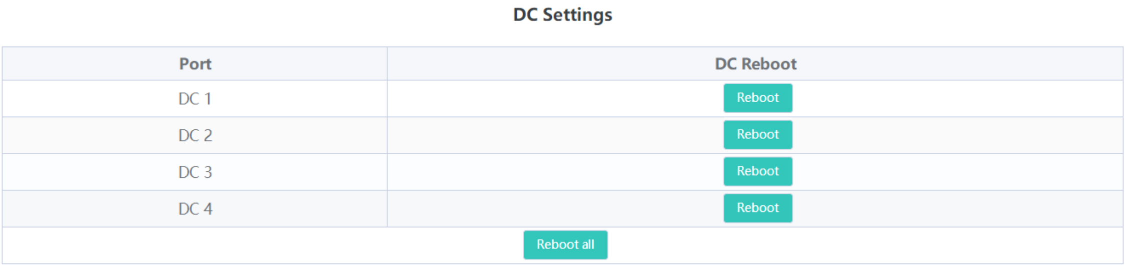
4.7 DC Port Reboot

⚠ **Caution**

Only RG-FS306-D switch supports this feature.

Choose **DC Settings**.

Select the DC port you want to reboot, and click **Reboot** to reboot the selected DC port. Click **Reboot all** to reboot all DC ports of the device.



DC Settings

Port	DC Reboot
DC 1	Reboot
DC 2	Reboot
DC 3	Reboot
DC 4	Reboot
Reboot all	

5 ES Series Switches Switch Settings

5.1 Managing MAC Address

5.1.1 Overview

The MAC address table records mappings of MAC addresses and ports to VLANs.

The device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC address in the packet, the device forwards the packet through the port specified by the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all ports other than the receiving port in broadcast mode.

MAC address entries are classified into the following types:

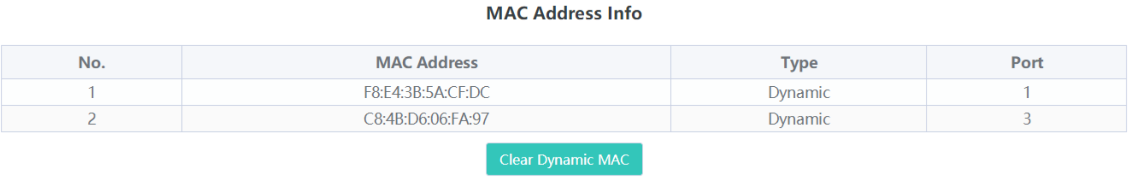
- Static MAC address entries: Static MAC address entries are manually configured by the users. Packets whose destination MAC address matches the one in such an entry are forwarded through the corresponding port.
- Dynamic MAC address entries: Dynamic MAC address entries are learned dynamically by the device. They are generated automatically by the device.

5.1.2 Viewing MAC Address Table

Choose **Switch Settings** > **MAC Address Info**.

This page displays the MAC address of the device, including the static MAC address configured manually by the users and the dynamic MAC address learned automatically by the device.

Click **Clear Dynamic MAC** to clear the dynamic MAC address learned by the device. The device will re-learn the MAC address and generate a MAC address table.



MAC Address Info

No.	MAC Address	Type	Port
1	F8:E4:3B:5A:CF:DC	Dynamic	1
2	C8:4B:D6:06:FA:97	Dynamic	3

Note

- If you disable VLAN, the device will forward packets according to only the destination MAC address. VLAN ID is not displayed in the MAC address table.
- Up to 100 MAC addresses are displayed.

5.1.3 Searching for MAC Address

Choose **Switch Settings** > **Search MAC**.

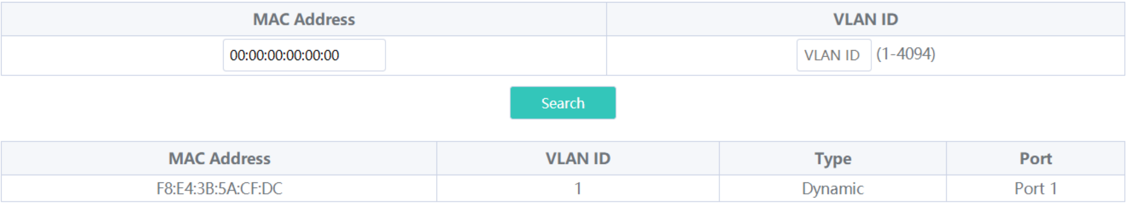
Users can search for MAC address entries according to MAC address and VLAN ID.

Caution

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table.MAC address entries can only be found through MAC address.

Enter MAC address and VLAN ID, and then click **Search**. The MAC address entries that meet the search criteria will be displayed in table right below the **Search** button. Moreover, users can enter partial characters of the MAC address for fuzzy search.

MAC Address Search



MAC Address	VLAN ID
00:00:00:00:00:00	VLAN ID (1-4094)

MAC Address	VLAN ID	Type	Port
F8:E4:3B:5A:CF:DC	1	Dynamic	Port 1

5.1.4 Configuring Static MAC Address

Choose **Switch Settings** > **Static MAC**.

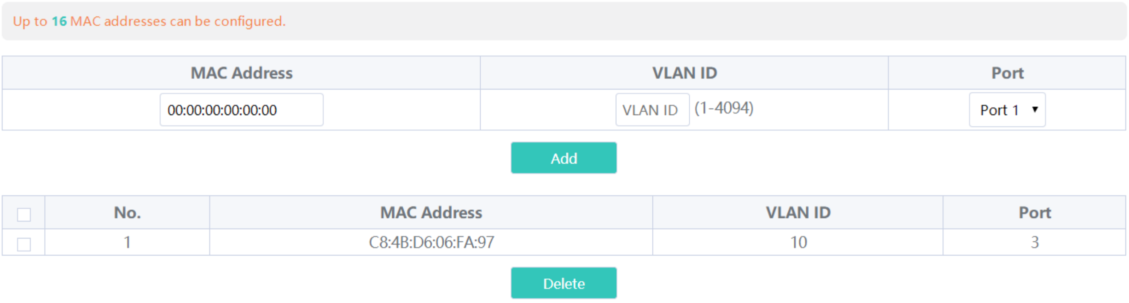
By configuring a static MAC address, users can manually bind the MAC address of a downlink network device with a port of the switch. After you add a static MAC address, when the device receives a packet destined to this address from VLAN, it forwards the packet to the specified port.

Caution

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table. It is not allowed to configure a VLAN to which the static MAC address belongs.

Enter a MAC address, specify a VLAN ID and select the outbound port. Then click **Add** to add a static MAC address. The MAC address entries will be updated accordingly in the MAC address table.

Static MAC Address

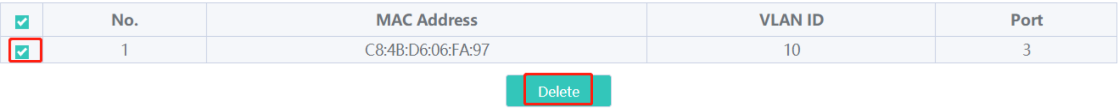


Up to 16 MAC addresses can be configured.

MAC Address	VLAN ID	Port
00:00:00:00:00:00	VLAN ID (1-4094)	Port 1 ▾

□	No.	MAC Address	VLAN ID	Port
□	1	C8:4B:D6:06:FA:97	10	3

If you want to delete a static MAC address, select the MAC address entry you want to delete in the table and click **Delete**.



☑	No.	MAC Address	VLAN ID	Port
☑	1	C8:4B:D6:06:FA:97	10	3

5.2 VLAN Settings

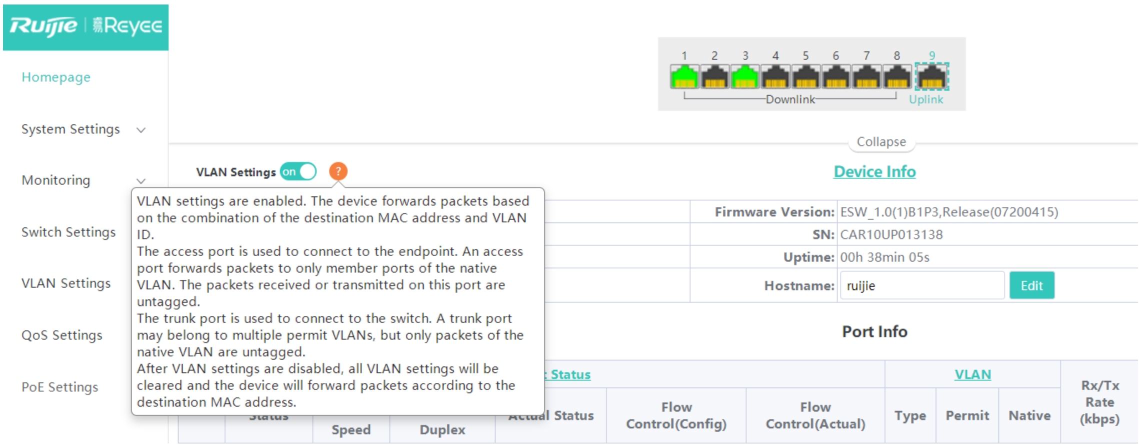
5.2.1 Global VLAN Settings

Choose **Homepage** > **Device Info**.

This page displays the status of VLAN settings. Toggle the **on-off** switch to enable or disable VLAN settings.

When VLAN is disabled, the device operates like an un-managed switch. The device forwards packets according to the destination MAC address, and the VLAN information of the forwarding packets remains unchanged during the forwarding process.

When VLAN is enabled, the device operates like a managed switch. The device forwards packets according to the destination MAC address and VLAN ID. Users can configure the port mode (access or trunk) based on whether a VLAN tag is carried in packets. Besides, all device ports will be initialized to access ports.



VLAN Settings on

VLAN settings are enabled. The device forwards packets based on the combination of the destination MAC address and VLAN ID.
The access port is used to connect to the endpoint. An access port forwards packets to only member ports of the native VLAN. The packets received or transmitted on this port are untagged.
The trunk port is used to connect to the switch. A trunk port may belong to multiple permit VLANs, but only packets of the native VLAN are untagged.
After VLAN settings are disabled, all VLAN settings will be cleared and the device will forward packets according to the destination MAC address.

Firmware Version: ESW_1.0(1)B1P3,Release(07200415)
SN: CAR10UP013138
Uptime: 00h 38min 05s
Hostname: ruijie Edit

	Status	Speed	Duplex	Actual Status	Flow Control(Config)	Flow Control(Actual)	VLAN Type	VLAN Permit	VLAN Native	Rx/Tx Rate (kbps)

5.2.2 Static VLANs Settings

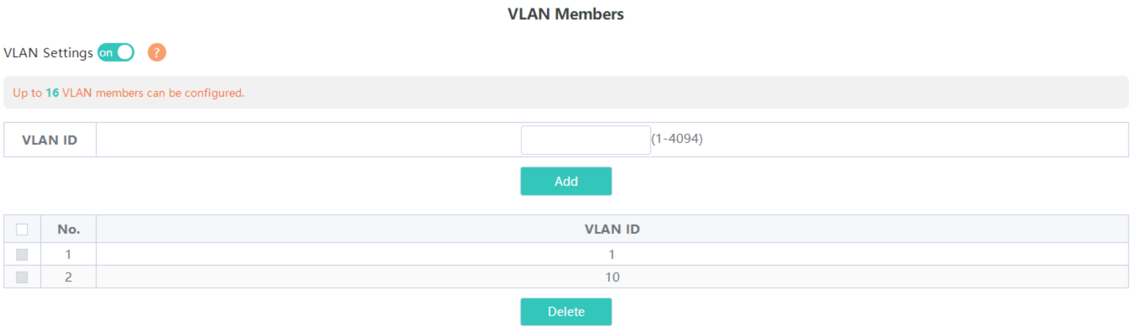
Caution

Static VLANs can be created only when the global VLAN settings feature is enabled. For details, see Chapter 3.2.1.

Choose **VLAN Settings** > **VLAN Members**.

Enter VLAN ID and click **Add** to create a static VLAN.

The VLAN table contains the existing VLANs. Select the VLANs and click **Delete**, and the corresponding VLANs will be deleted. VLAN 1 cannot be deleted.


VLAN Members

VLAN Settings on

Up to 16 VLAN members can be configured.

VLAN ID (1-4094)

Add

□	No.	VLAN ID
□	1	1
□	2	10

Delete

Note

- The VLAN ID ranges from 1 to 4094. VLAN 1 is the default VLAN.
- The default VLAN (VLAN 1), Management VLAN, Native VLAN, Permit VLAN, and Access VLAN cannot be deleted.

5.2.3 Port VLAN Settubgs

Caution

Users can configure port VLAN only when the global VLAN settings feature is enabled. For details, see Chapter 3.2.1.

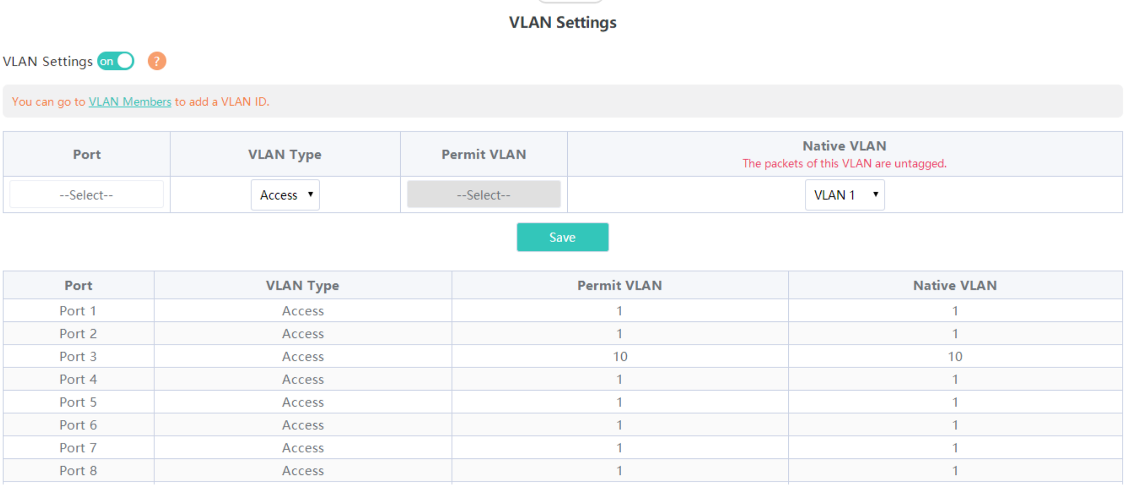
Choose **VLAN Settings** > **VLAN Settings**.

Configure the port mode and VLAN members of a port, and you will know the allowed VLANs of the port and whether the packets forwarded by the port carry tags.

Note

You are advised to create VLAN members (refer to Chapter 3.2.2) before configuring the port based on VLANs. Click **VLAN Members** to access **VLAN Members** page where you can add VLAN members.

Select the port you want to configure and the port mode. If you select the access mode, select **Access VLAN** for the port and click **Save**. If you select the trunk mode, select **Native VLAN** for the port and enter the VLAN ID range allowed by the port and click **Save**.



VLAN Settings

VLAN Settings on ?

You can go to VLAN Members to add a VLAN ID.

Port	VLAN Type	Permit VLAN	Native VLAN The packets of this VLAN are untagged.
--Select--	Access ▾	--Select--	VLAN 1 ▾

Save

Port	VLAN Type	Permit VLAN	Native VLAN
Port 1	Access	1	1
Port 2	Access	1	1
Port 3	Access	10	10
Port 4	Access	1	1
Port 5	Access	1	1
Port 6	Access	1	1
Port 7	Access	1	1
Port 8	Access	1	1

Table 5-1 Port Modes

Port Mode	Description

Access	One access port can belong to only one VLAN and allow frames from this VLAN only to pass through. This VLAN is called an access VLAN. The frames from the access port do not carry VLAN tag. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame. Access port is connected to the endpoints.
Trunk	One trunk port supports one Native VLAN and several Permit VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while Permit VLAN frames forwarded by the trunk port carry tags. Trunk port is connected to switches. Users can set the Permit VLAN range to limit VLAN frames that can be forwarded. Make sure the trunk ports at the two ends of the link are configured with the same Native VLAN.

Note

Improper configuration of VLANs on a port (especially uplink port) may cause failure to log in to the web management system. Exercise caution when configuring VLANs.

6 ES Series Switches Security

6.1 DHCP Snooping

6.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server.

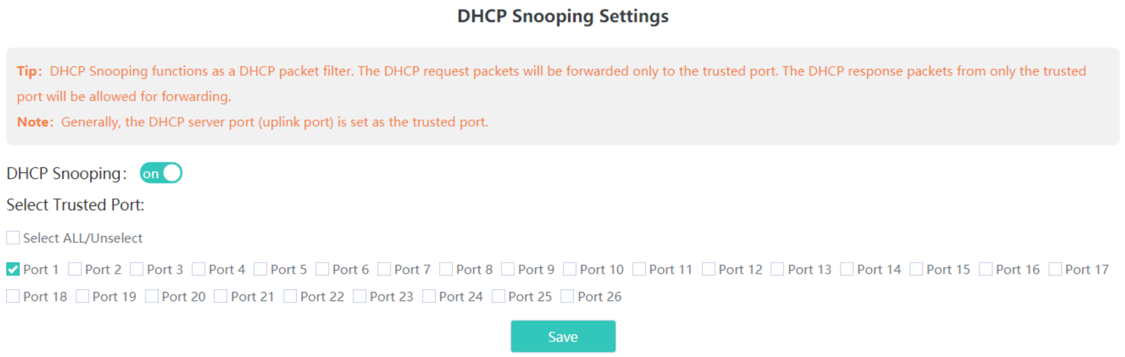
6.1.2 Configuration Steps

Choose **Switch Settings** > **DHCP Snooping Settings**.

Toggle the switch to **On** to enable DHCP snooping,   select the trusted ports, and then click **Save**. When DHCP snooping is enabled, request packets from DHCP clients are forwarded only to the trusted ports. For response packets from DHCP servers, only those from the trusted ports are forwarded.

Note

The uplink port connected to the DHCP server is configured as the trusted port generally.



DHCP Snooping Settings

Tip: DHCP Snooping functions as a DHCP packet filter. The DHCP request packets will be forwarded only to the trusted port. The DHCP response packets from only the trusted port will be allowed for forwarding.

Note: Generally, the DHCP server port (uplink port) is set as the trusted port.

DHCP Snooping: on

Select Trusted Port:

□ Select ALL/Unselect

☑ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5 □ Port 6 □ Port 7 □ Port 8 □ Port 9 □ Port 10 □ Port 11 □ Port 12 □ Port 13 □ Port 14 □ Port 15 □ Port 16 □ Port 17

□ Port 18 □ Port 19 □ Port 20 □ Port 21 □ Port 22 □ Port 23 □ Port 24 □ Port 25 □ Port 26

6.2 Storm Control

6.2.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

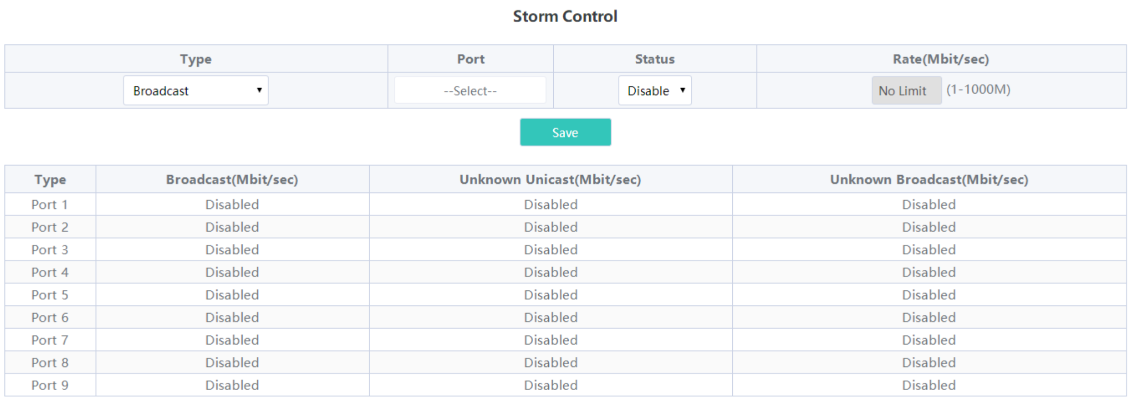
Users can perform storm control separately for the broadcast, unknown multicast, and unknown unicast data flows. When the rate of broadcast, unknown multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

6.2.2 Configuration Steps

Choose **QoS Settings** > **Storm Control**.

Select the storm control type, port, status, and enter the rate limit, and then click **Save**.

The storm control type and corresponding rate are displayed in the table right below the **Save** button. When storm control is disabled, the rate of broadcast, unknown multicast, and unknown unicast data flows is not limited. The corresponding status is displayed **Disabled**. When storm control is enabled, the corresponding rate limits will be displayed.



Storm Control

Type	Port	Status	Rate(Mbit/sec)
Broadcast ▾	--Select--	Disable ▾	No Limit (1-1000M)

Type	Broadcast(Mbit/sec)	Unknown Unicast(Mbit/sec)	Unknown Broadcast(Mbit/sec)
Port 1	Disabled	Disabled	Disabled
Port 2	Disabled	Disabled	Disabled
Port 3	Disabled	Disabled	Disabled
Port 4	Disabled	Disabled	Disabled
Port 5	Disabled	Disabled	Disabled
Port 6	Disabled	Disabled	Disabled
Port 7	Disabled	Disabled	Disabled
Port 8	Disabled	Disabled	Disabled
Port 9	Disabled	Disabled	Disabled

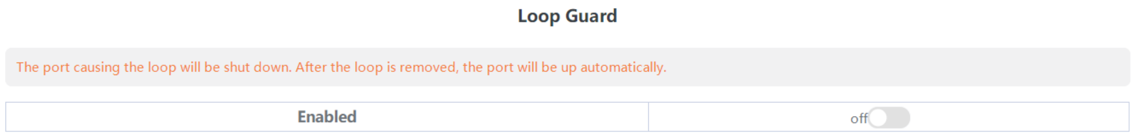
Note

- The rate limit for the ports of RG-ES205C-P switch ranges from 1Mpbs to 100Mbps.
- The maximum rate supported by ports 1 to 8 of RG-ES209C-P switch is 100Mbps. If the configured rate exceeds 100Mbps, the effective rate will still be 100Mbps. The rate limit for port 9 ranges from 1Mbps to 1000Mbps.
- The rate limit for the ports of RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P, RG-FS306-D switches ranges from 1Mbps to 1000Mbps.

6.3 Loop Guard

Choose **Monitoring** > **Loop Guard**.

When loop guard feature is enabled, the port causing the loop will be shut down automatically. After the loop is removed, the port will be up automatically. Loop guard function is disabled by default.



Loop Guard

The port causing the loop will be shut down. After the loop is removed, the port will be up automatically.

Enabled	off

7 ES Series Switches PoE Settings

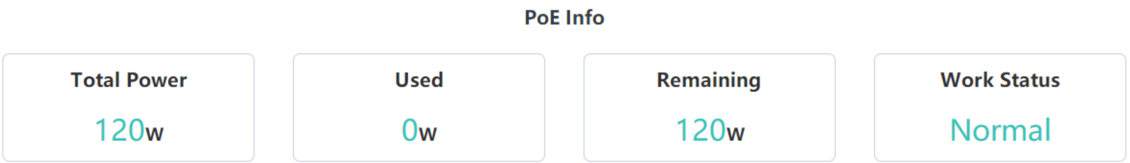
Caution

Only RG-ES226GC-P, RG-ES218GC-P, RG-ES209GC-P, RG-ES209C-P, RG-ES205GC-P, RG-ES205C-P, and RG-FS306-P switches support the PoE function.

Choose **PoE Settings**.

The device supports PoE power supply. Users can view and configure the current power status.

Device status: The total power, used power, remaining power, and current work status of the PoE system are displayed.

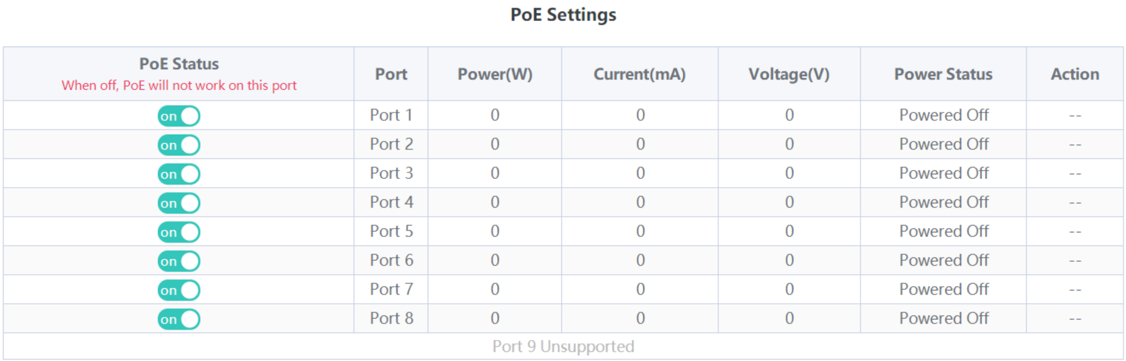


PoE Info

Total Power	Used	Remaining	Work Status
120w	0w	120w	Normal

Port status: The voltage, current, output power, and current power status of the device ports are displayed. Users can enable or disable PoE function through the **on-off** toggle switch. When PoE is disabled, the port will not supply power to external devices.

If a PD device fails, please power on the port connected to the PD device again to reboot it.



PoE Settings

PoE Status When off, PoE will not work on this port	Port	Power(W)	Current(mA)	Voltage(V)	Power Status	Action
on	Port 1	0	0	0	Powered Off	--
on	Port 2	0	0	0	Powered Off	--
on	Port 3	0	0	0	Powered Off	--
on	Port 4	0	0	0	Powered Off	--
on	Port 5	0	0	0	Powered Off	--
on	Port 6	0	0	0	Powered Off	--
on	Port 7	0	0	0	Powered Off	--
on	Port 8	0	0	0	Powered Off	--

Port 9 Unsupported

Note

The fiber ports of RG-ES226GC-P, RG-ES218GC-P, and RG-FS306-P switches do not support the PoE function.

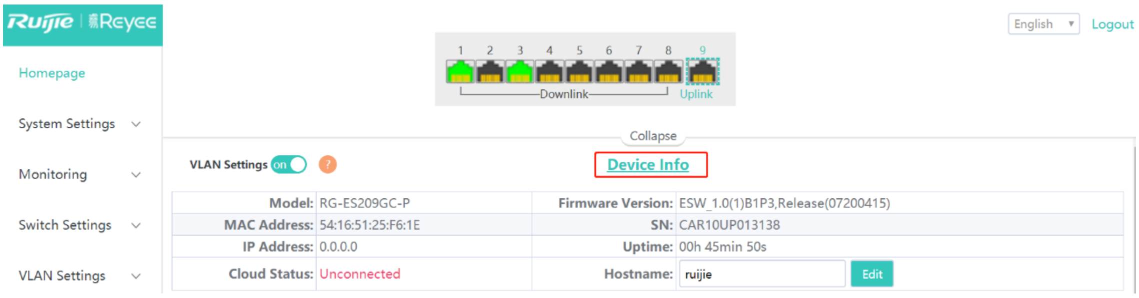
8 ES Series Switches System Settings

8.1 Managing Device Information

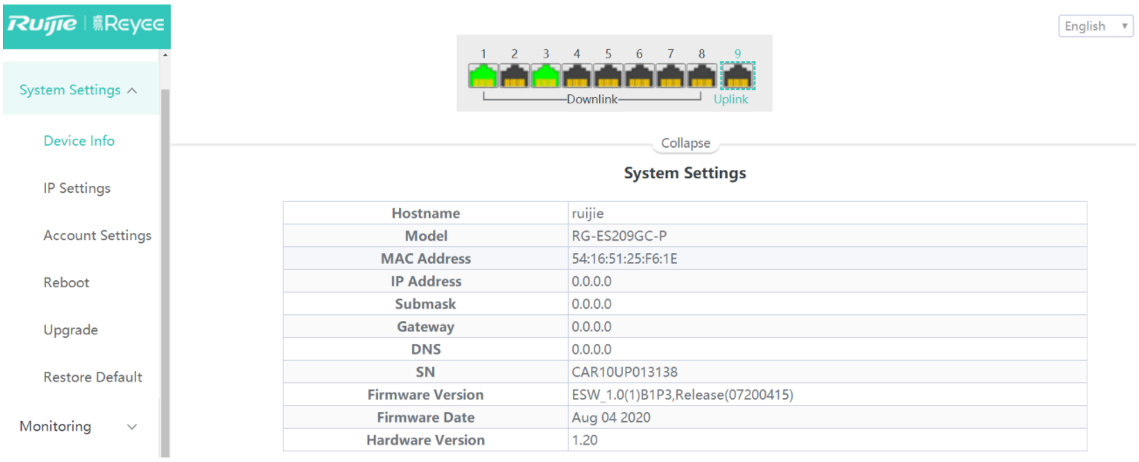
8.1.1 Viewing Device Information

Choose **Homepage** > **Device Info**.

The device information is displayed on the homepage, including hostname, device model, serial number, firmware version, IP address, MAC address, cloud status, and uptime. Click **Device Info** to access the **Device Info** page (**System Settings** > **Device Info**) to view more detailed information.



Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)
MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138
IP Address:	0.0.0.0	Uptime:	00h 45min 50s
Cloud Status:	Unconnected	Hostname:	ruijie



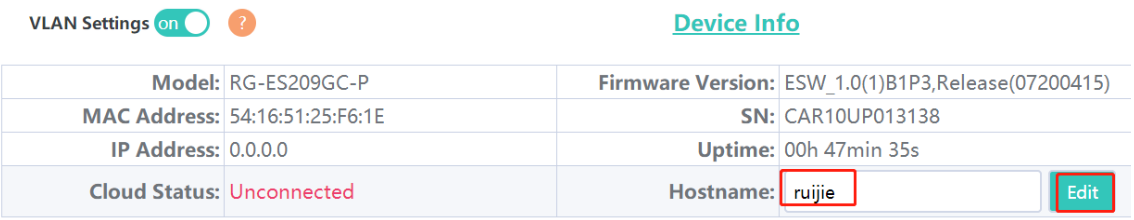
System Settings

Hostname	ruijie
Model	RG-ES209GC-P
MAC Address	54:16:51:25:F6:1E
IP Address	0.0.0.0
Submask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
SN	CAR10UP013138
Firmware Version	ESW_1.0(1)B1P3,Release(07200415)
Firmware Date	Aug 04 2020
Hardware Version	1.20

8.1.2 Editing the Hostname

Choose **Homepage** > **Device Info**.

Enter the hostname and click **Edit** to edit the hostname in order to distinguish different devices.

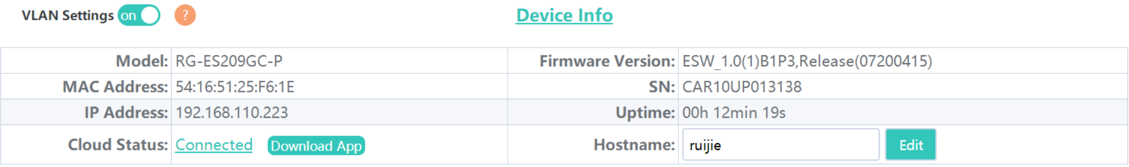


Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)
MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138
IP Address:	0.0.0.0	Uptime:	00h 47min 35s
Cloud Status:	Unconnected	Hostname:	ruijie

8.1.3 Cloud Management

Choose **Homepage** > **Device Info**.

Cloud status displays whether the device is connected to the cloud. After the device is bound to a cloud management account, the Cloud Status will display **Connected**, and users can manage the device remotely through Ruijie Cloud webpage or APP. Click **Connected** to access the homepage of Ruijie Cloud (https://cloud-as.ruijienetworks.com). Click **Download APP** to download Ruijie Cloud APP.



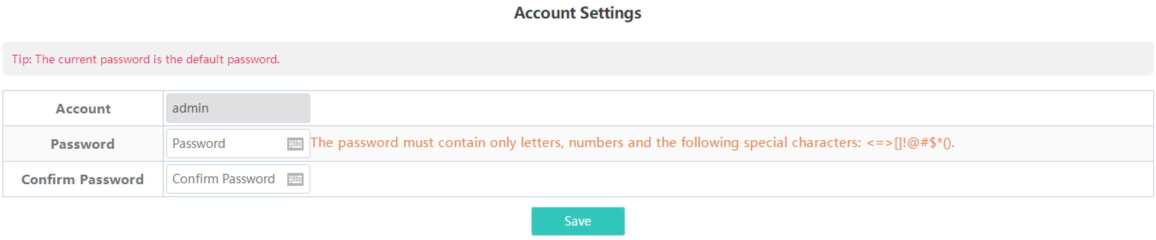
Device Info

Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)
MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138
IP Address:	192.168.110.223	Uptime:	00h 12min 19s
Cloud Status:	Connected Download App	Hostname:	ruijie Edit

8.2 Password Settings

When the device password is the default password, users will be prompted to reset the password when they log into the Eweb management system. Click **Yes** to access the **Account Settings** page (or choose **System Settings** > **Account Settings** to access the page).

Set a new password according to the tip, and then click **Save** to save the configuration.

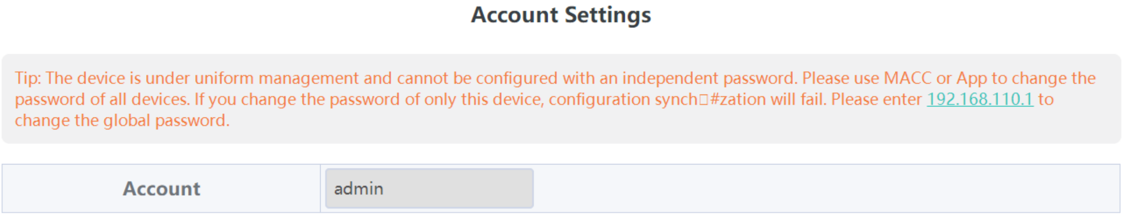


Account Settings

Tip: The current password is the default password.

Account	admin	
Password	Password	The password must contain only letters, numbers and the following special characters: <=>[]!@#$*().
Confirm Password	Confirm Password	

If the device is under uniform management, it cannot be configured with an independent password. Users need to follow the tip to log in to the master device for global password configuration.



Account Settings

Tip: The device is under uniform management and cannot be configured with an independent password. Please use MACC or App to change the password of all devices. If you change the password of only this device, configuration synch□#zation will fail. Please enter 192.168.110.1 to change the global password.

Account	admin

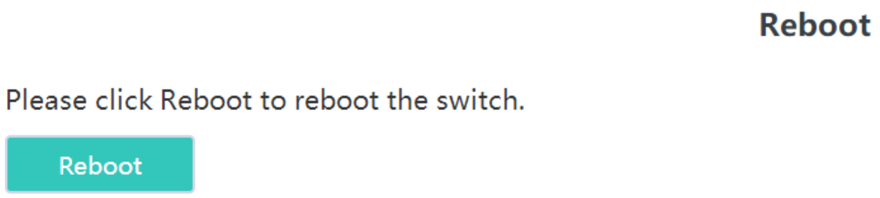
Caution

- Upon your initial login to the Eweb management system, you must set the device management password first before you configuring other features.
- Please remember the device management password (default username/password: admin/admin). You may need to log in again after changing the password.
- If the device has been under uniform management, please use MACC or APP to change the network-wide password. Changing the password of this device will cause failure to synchronize network-wide settings to this device.

8.3 Device Reboot

Choose **System Settings** > **Reboot**.

Click **Reboot** to reboot the switch.


Reboot

Please click Reboot to reboot the switch.

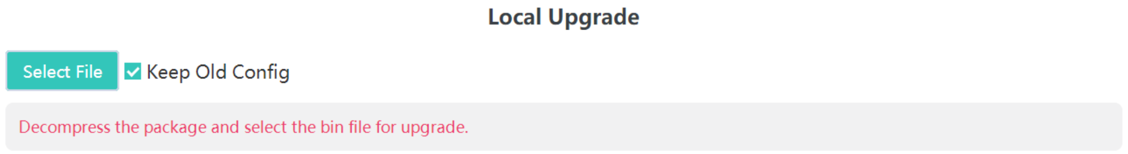
8.4 System Upgrade

8.4.1 Local Upgrade

Choose **System Settings** > **Upgrade**.

Click **Select File** to select the upgrade package from the local files (the upgrade package is a bin file. If it is a tar.gz file, users need to decompress the package and select the bin file for upgrade).

Keep Old Config is selected by default. That means the current configuration will be saved after device upgrade. If there is a huge difference between the current version and the upgrade version, you are advised not to select **Keep Old Config**.


Local Upgrade

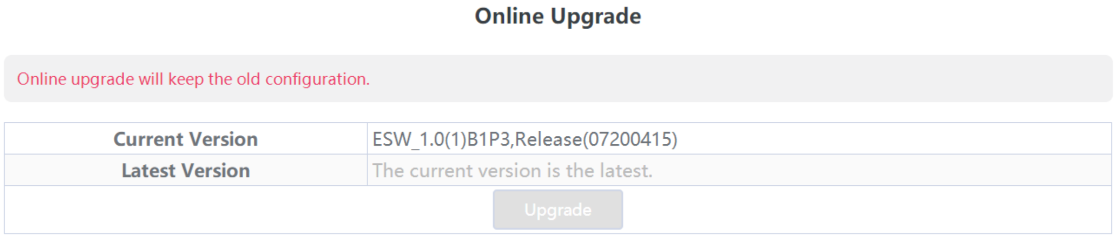
☑ Keep Old Config

Decompress the package and select the bin file for upgrade.

8.4.2 Online Upgrade

Choose **System Settings** > **Upgrade**.

When there is a new version in the cloud, the version number of the latest version will be displayed on this page, and the **Upgrade** button will become available. The device will download the installation package of the recommended version from the cloud and it will be updated to the latest version. Online upgrade will keep the old configuration by default.


Online Upgrade

Online upgrade will keep the old configuration.

Current Version	ESW_1.0(1)B1P3,Release(07200415)
Latest Version	The current version is the latest.

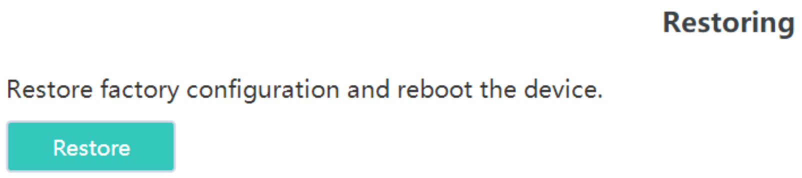
Note

The time that online upgrade takes depends on the current network speed. It may take some time. Please be patient.

8.5 Restoring Factory Configuration

Choose **System Settings** > **Restore Default**.

Click **Restore** to restore factory configuration and reboot the device.



Restoring

Restore factory configuration and reboot the device.

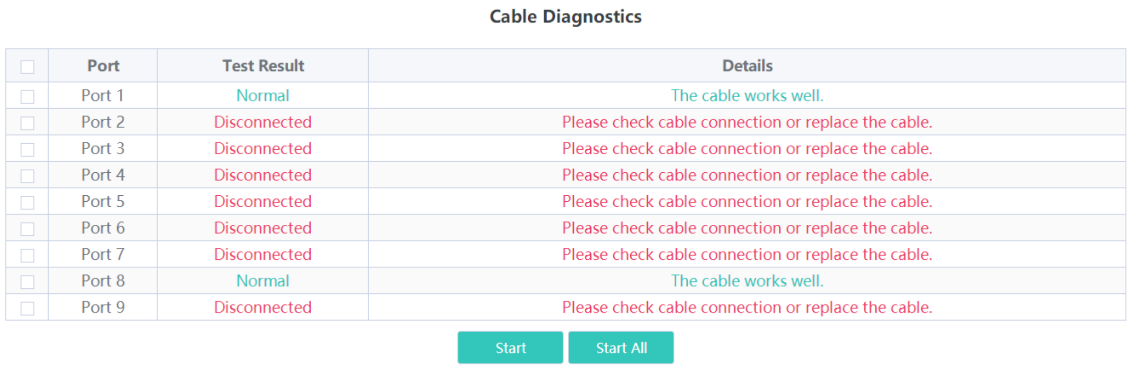
9 ES Series Switches Monitoring

9.1 Cable Diagnostics

Choose **Monitoring** > **Cable Diagnostics**.

Cable diagnostics allows users to check the status of Ethernet cables. For example, users can check whether the cables are short-circuited or disconnected.

Select the ports you want to detect, and then click **Start** to start cable diagnostics. The test result will be displayed accordingly. Click **Start All** to perform one-click cable diagnostics on all ports.



Cable Diagnostics

□	Port	Test Result	Details
□	Port 1	Normal	The cable works well.
□	Port 2	Disconnected	Please check cable connection or replace the cable.
□	Port 3	Disconnected	Please check cable connection or replace the cable.
□	Port 4	Disconnected	Please check cable connection or replace the cable.
□	Port 5	Disconnected	Please check cable connection or replace the cable.
□	Port 6	Disconnected	Please check cable connection or replace the cable.
□	Port 7	Disconnected	Please check cable connection or replace the cable.
□	Port 8	Normal	The cable works well.
□	Port 9	Disconnected	Please check cable connection or replace the cable.

⚠ **Caution**

If you select an uplink port for diagnostics, the network may be intermittenly disconnected. Exercise caution when performing this operation.

9.2 Multi-DHCP Alarming

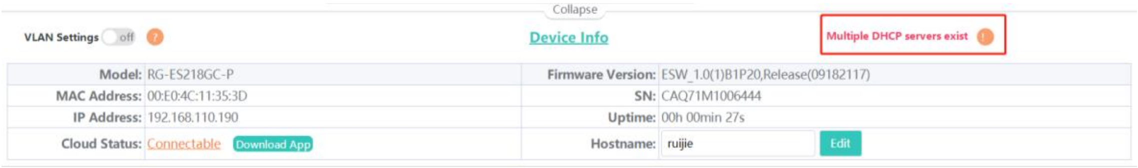
⚠ **Caution**

- Only RG-ES226GC-P, RG-ES218GC-P, RG-ES224GC, RG-ES216GC switches support multi-DHCP alarming.

- Multi-DHCP alarming will fail when the device IP address is not obtained dynamically. For relevant IP address configuration, see Chapter 2.6.

Choose **Homepage**.

When there are multiple DHCP servers in a LAN, the system will send a conflicting alarm. An alarming message will be displayed in the **Device Info** column.



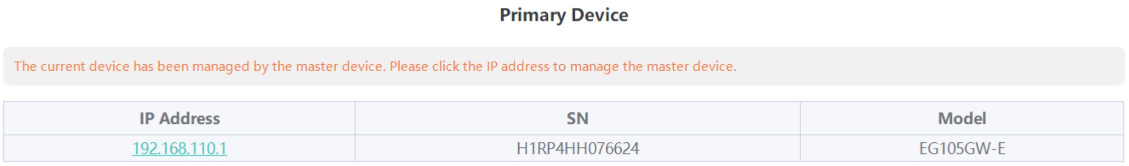
Model:	RG-ES218GC-P	Firmware Version:	ESW_1.0(1)B1P20,Release(09182117)
MAC Address:	00:E0:4C:11:35:3D	SN:	CAQ71M1006444
IP Address:	192.168.110.190	Uptime:	00h 00min 27s
Cloud Status:	Connectable	Hostname:	ruijie

Move the cursor to ? to view the alarm details, including the VLAN where the conflicts occur, port, IP address of DHCP server, and MAC address.

9.3 Viewing Switch Information

Choose **Monitoring** > **Switches**.

If the switch is under uniform management, some features cannot be configured independently (such as password settings). To facilitate configuration, information of the master device in the VLAN will be displayed in this page. Click the **IP Address** of the master device to access **Master Device** page for global configuration.



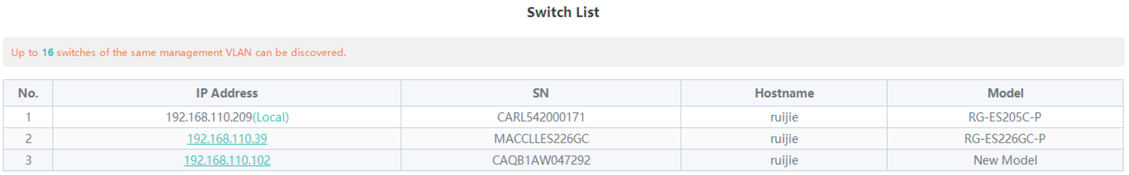
Primary Device

The current device has been managed by the master device. Please click the IP address to manage the master device.

IP Address	SN	Model
192.168.110.1	H1RP4HH076624	EG105GW-E

The device is able to automatically discover other switches in the same management VLAN. Information of these switches will be displayed in **Switch List**.

The first row of **Switch List** displays information of the current device, and the following rows display information of other devices. Click **IP Address** of a device to access the Eweb management system of the device (login required).



Switch List

Up to 16 switches of the same management VLAN can be discovered.

No.	IP Address	SN	Hostname	Model
1	192.168.110.209(Local)	CARL542000171	ruijie	RG-ES205C-P
2	192.168.110.39	MACCLLES226GC	ruijie	RG-ES226GC-P
3	192.168.110.102	CAQB1AW047292	ruijie	New Model

Note

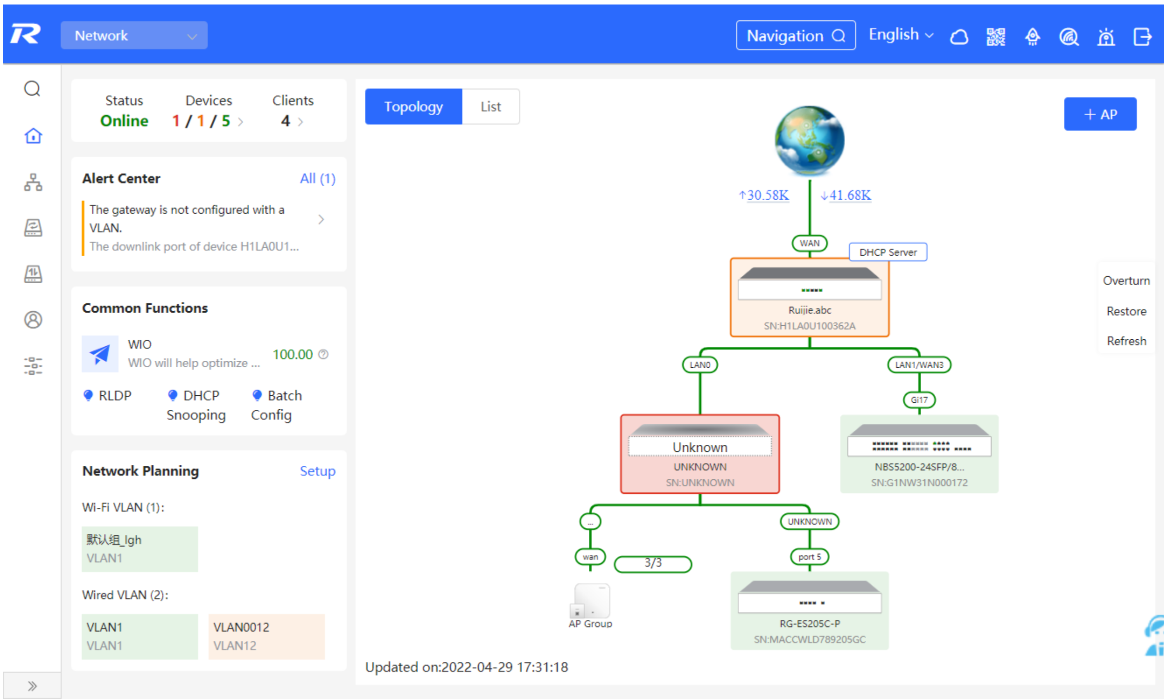
The number of switches that can be discovered varies with product modes:

- RG-ES226GC-P, RG-ES218GC-P and RG-FS303-AB can discover 32 switches.
- RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, RG-ES209GC-P, RG-FS306-P and RG-FS306-D can discover 16 switches.

10 NBS Series Network management

10.1 Overviewing Network Information

In network mode, the **Overview** page displays the current network topology, uplink and downlink real-time traffic, network connection status, and number of users and provides short-cut entries for configuring the network and devices. Users can monitor and manage the network status of the entire network on the page.



Status Online
Devices 1 / 1 / 5
Clients 4

Alert Center All (1)
The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...

Common Functions
WIO
WIO will help optimize ... 100.00

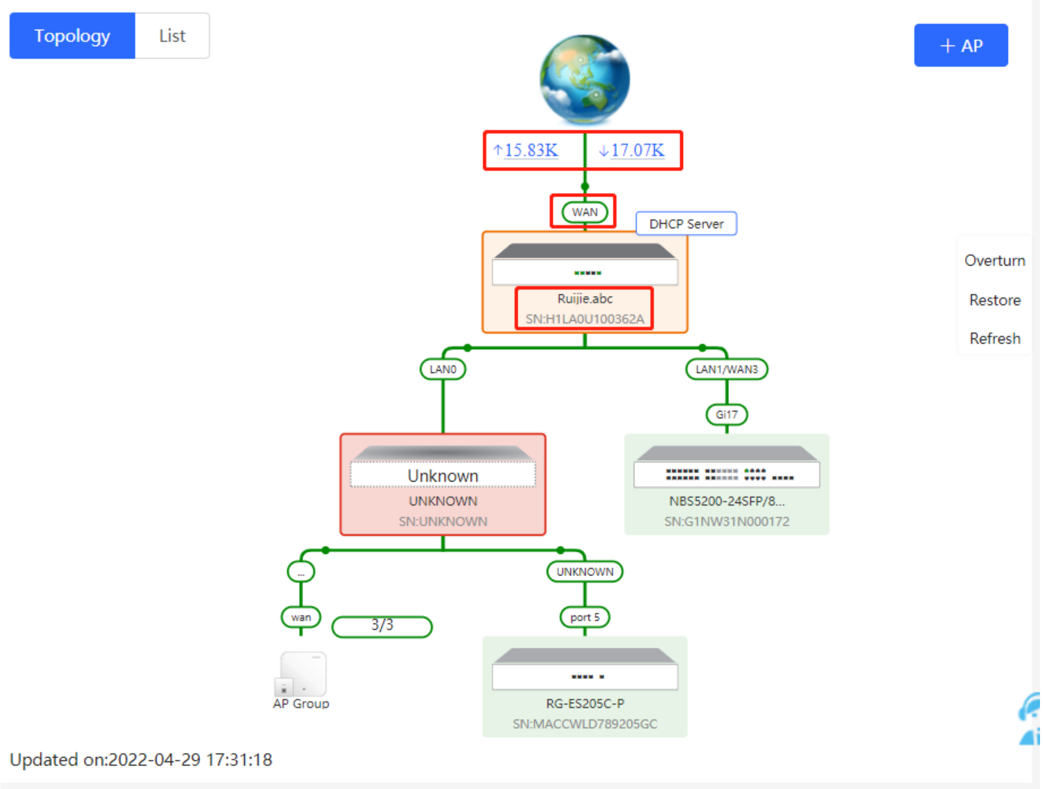
Network Planning Setup
Wi-Fi VLAN (1):
默认组_lgh VLAN1
Wired VLAN (2):
VLAN1 VLAN1
VLAN0012 VLAN12

Updated on:2022-04-29 17:31:18

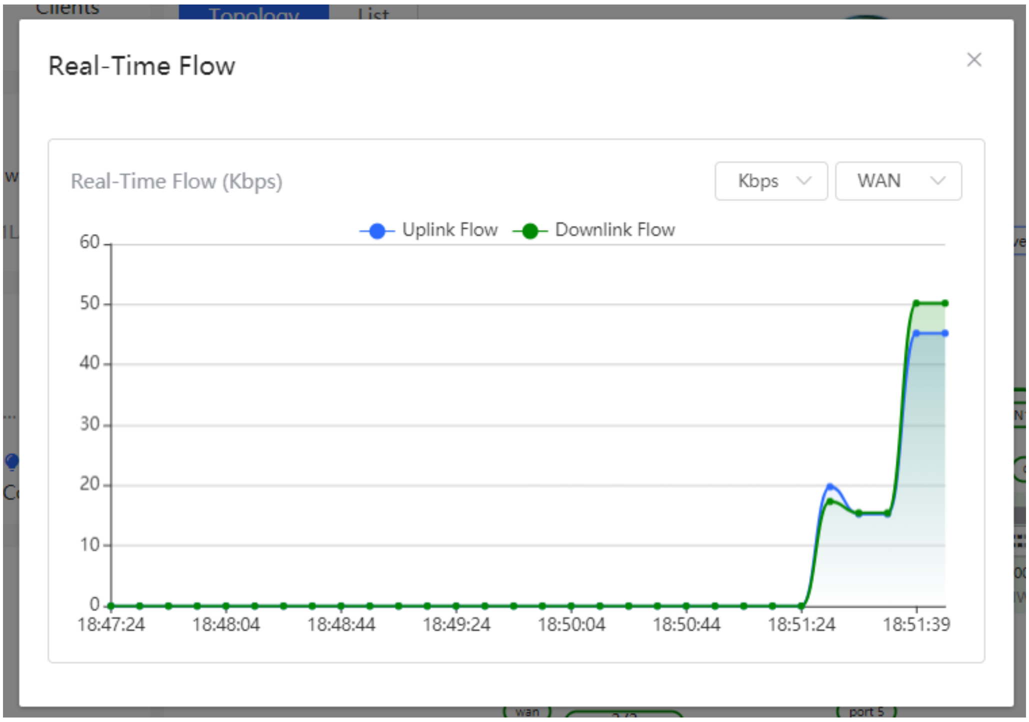
10.2 Viewing Networking Information

Choose **Network** > **Overview**.

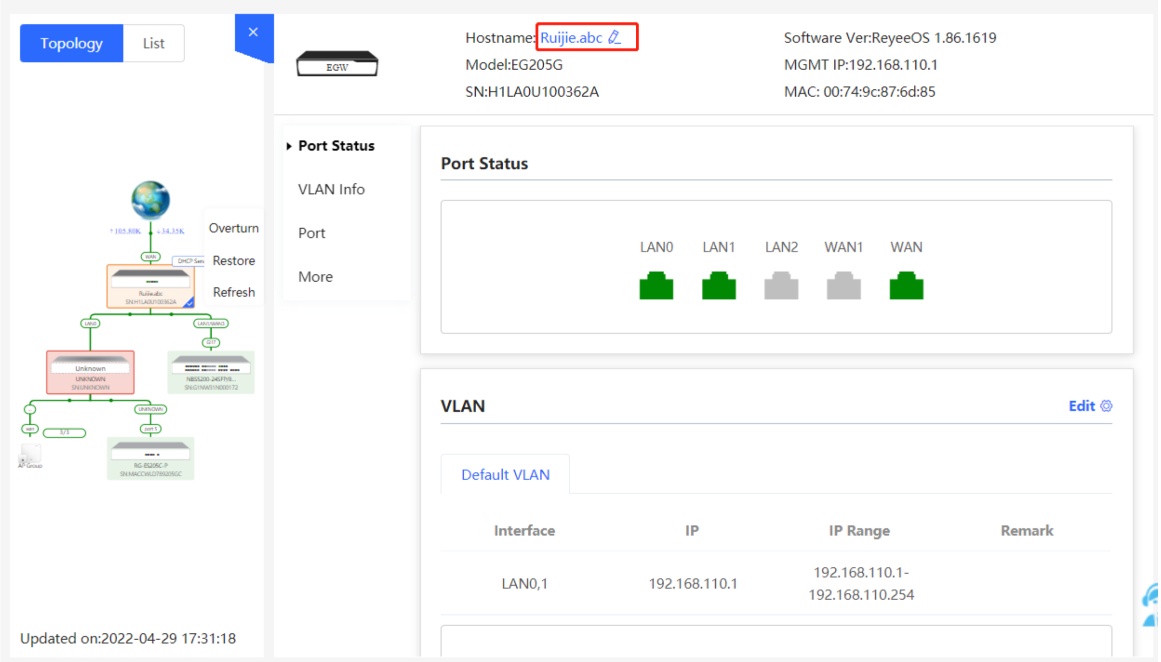
The networking topology contains information about online devices, connected port numbers, device SNs, and uplink and downlink real-time traffic.



- Click a traffic data item to view the real-time total traffic information.



- Click a device in the topology to view the running status and configuration of the device and configure device functions. By default, the product model is used as the device name. Click 🖉 to modify the device name so that the description can distinguish devices from one another.



Hostname: Ruijie.abc

Model:EG205G

SN:H1LA0U100362A

Software Ver:ReyeeOS 1.86.1619

MGMT IP:192.168.110.1

MAC: 00:74:9c:87:6d:85

- Port Status
- VLAN Info
- Port
- More

Port Status

LAN0	LAN1	LAN2	WAN1	WAN
🟩	🟩	▨	▨	🟩

VLAN

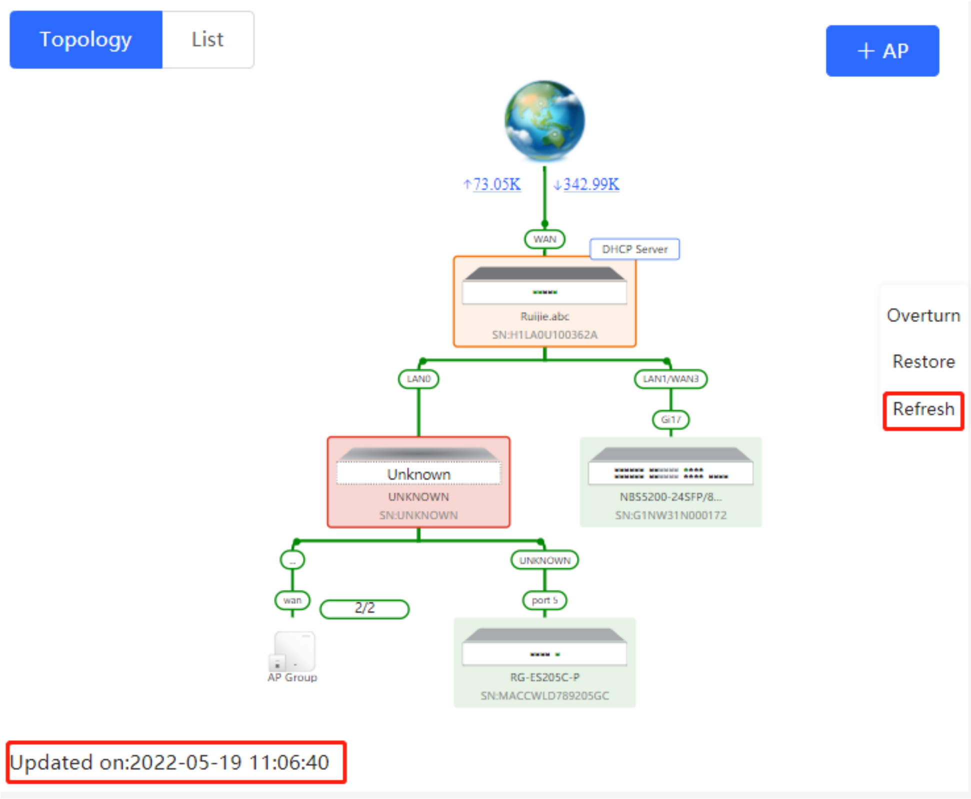
Edit

Default VLAN

Interface	IP	IP Range	Remark
LAN0,1	192.168.110.1	192.168.110.1- 192.168.110.254	

Updated on:2022-04-29 17:31:18

- The update time is displayed in the lower-left corner of the topology view. Click **Refresh** to update the topology to the latest state. It takes some time to update the topology data. Please wait patiently.

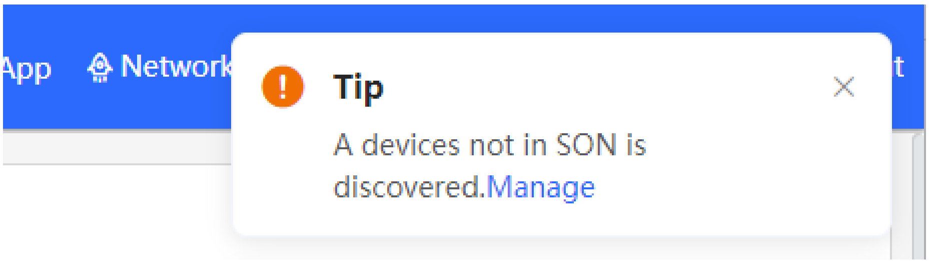


Updated on:2022-05-19 11:06:40

10.3 Adding Networking Devices

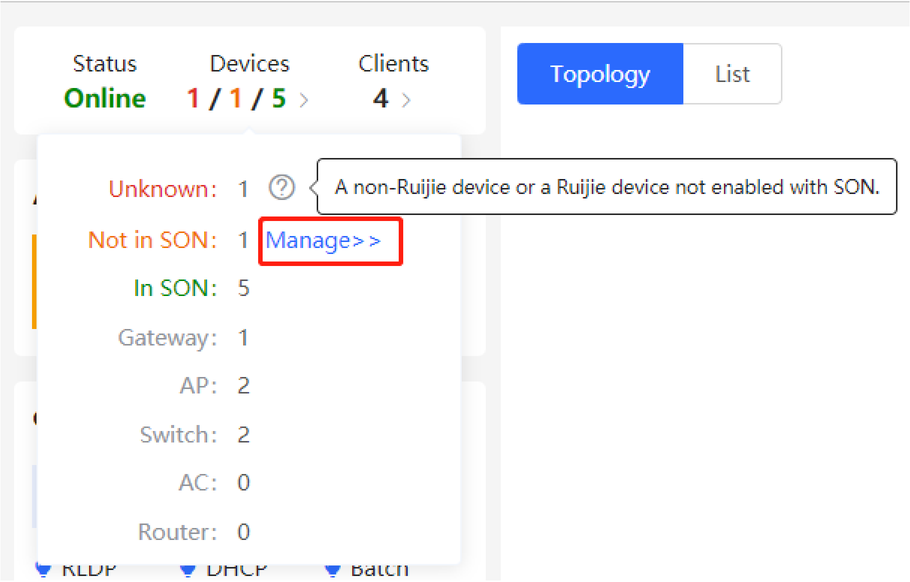
10.3.1 Wired Connection

(1) When a new device connects to an existing device on the network, the system displays the message “A device not in SON is discovered.” and the number of such devices in orange under “Devices” on the upper-left corner of the [Overview] page. You can click **Manage** to add this device to the current network.



Tip

A devices not in SON is discovered.Manage



Status Online

Devices 1 / 1 / 5 >

Clients 4 >

Unknown: 1

A non-Ruijie device or a Ruijie device not enabled with SON.

Not in SON: 1 Manage>>

In SON: 5

Gateway: 1

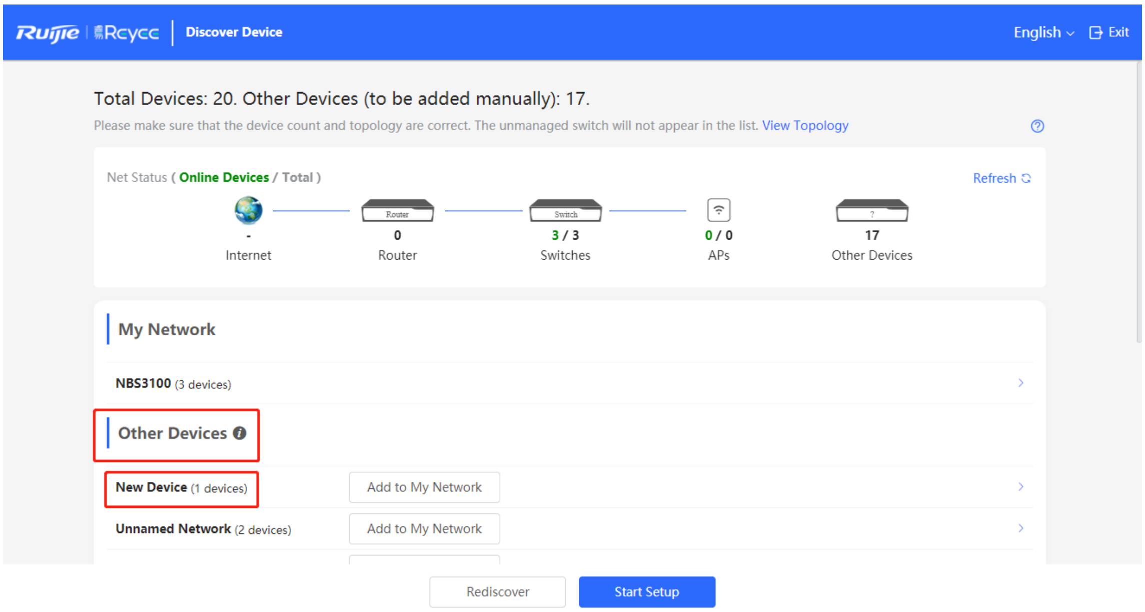
AP: 2

Switch: 2

AC: 0

Router: 0

(2) After the system switches to the **Network List** page, click **Other Network**. In the **Other Network** section, select the device to be added to the network and click **Add to My Network**.



Ruijie | Rcycc | Discover Device English Exit

Total Devices: 20. Other Devices (to be added manually): 17.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. View Topology

Net Status (Online Devices / Total) Refresh

Internet	Router	Switches	APs	Other Devices
-	0	3 / 3	0 / 0	17

My Network

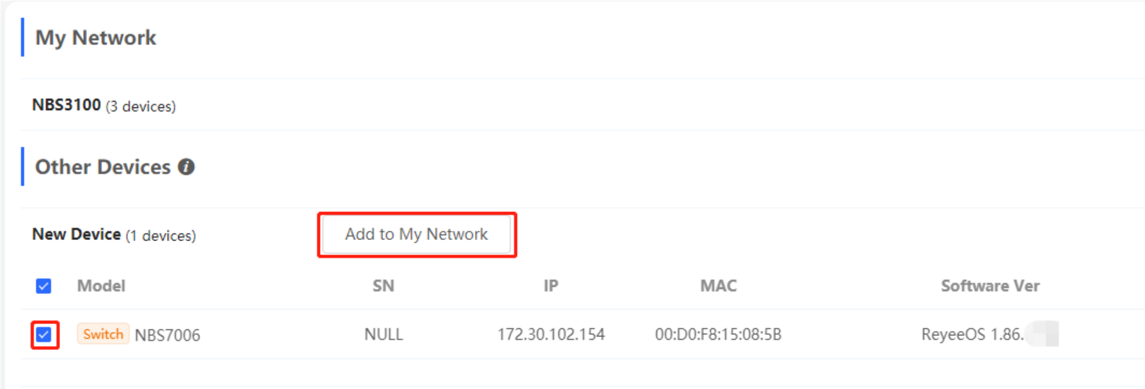
NBS3100 (3 devices)

Other Devices

New Device (1 devices) Add to My Network

Unnamed Network (2 devices) Add to My Network

Rediscover Start Setup



My Network

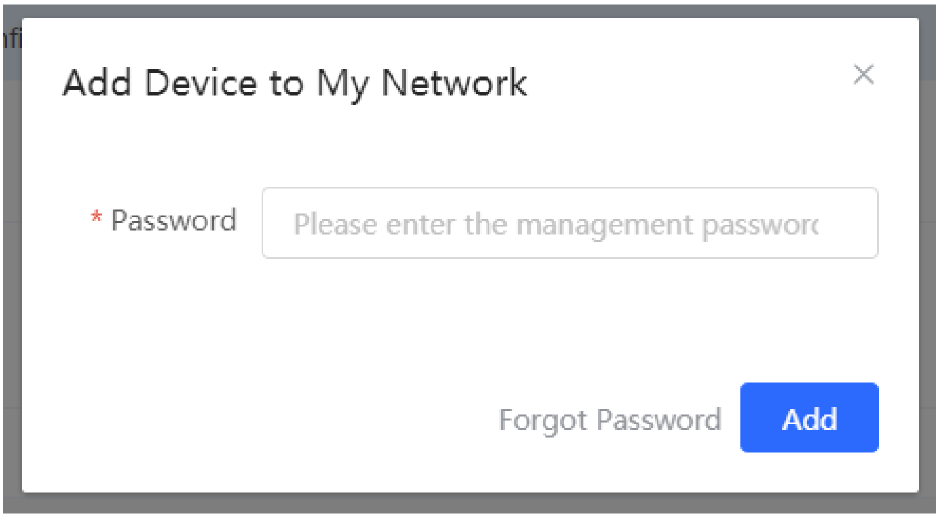
NBS3100 (3 devices)

Other Devices

New Device (1 devices) Add to My Network

☑	Model	SN	IP	MAC	Software Ver
☑	Switch NBS7006	NULL	172.30.102.154	00:D0:F8:15:08:5B	ReyeeOS 1.86.

(3) You do not need to enter the password if the device to add is newly delivered from factory. If the device has a password, enter the configuring password of the device. Device addition fails if the password is incorrect.



Add Device to My Network

* Password Please enter the management passworc

Forgot Password Add

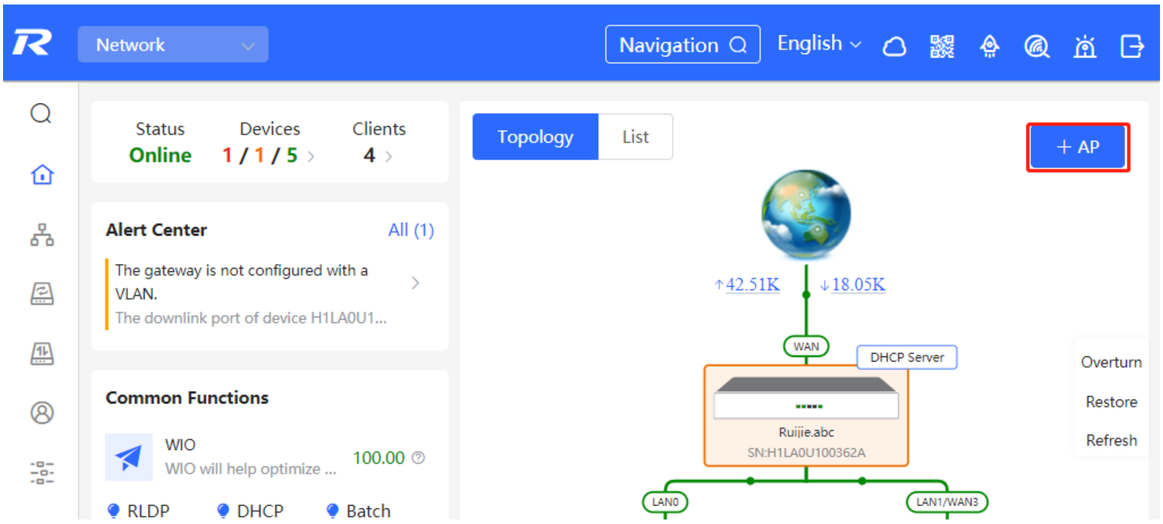
10.3.2 AP Mesh

If the AP supports the AP Mesh (Reyee Mesh) function, you do not need to connect cables after powering on the AP. The AP can be added to the current network in Reyee Mesh mode, establish a mesh networking with other wireless devices, and automatically synchronize Wi-Fi configuration.

Caution

To scan the AP, the Reyee Mesh function must be enabled on the current network. (For details, see 0.) The AP should be powered on nearby. It may fail to be scanned in case of long distance or obstacle blocking.

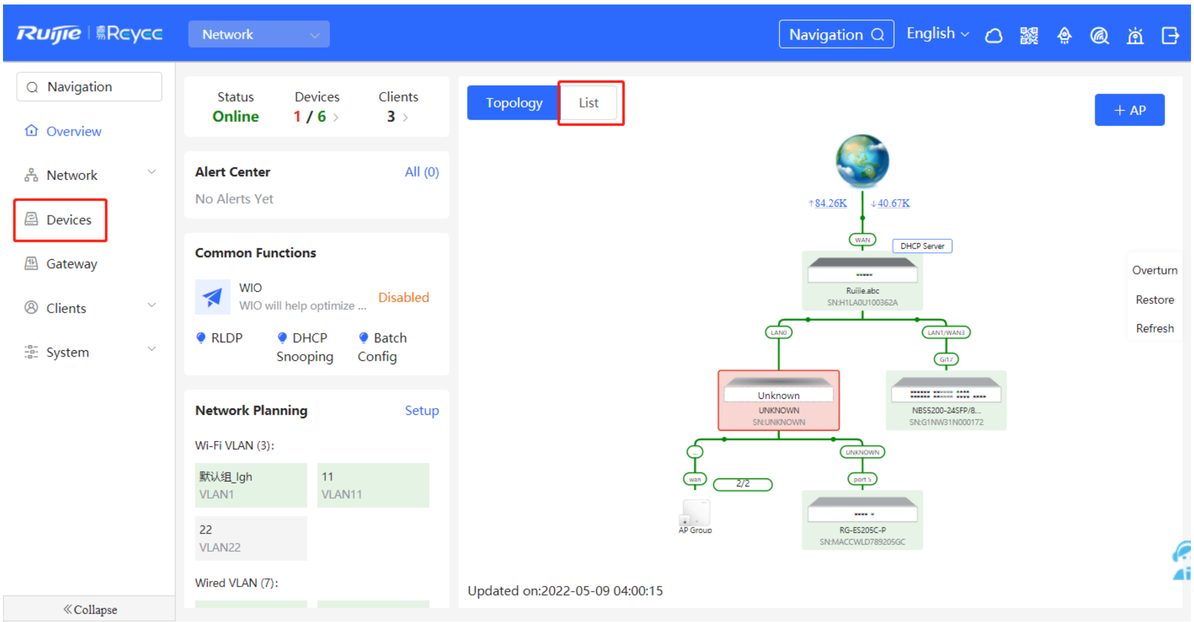
(1) Place the powered new AP near an existing AP, where the new AP can receive Wi-Fi signals from the existing AP. Log in to a device in the network. On the **Overview** page, click **+AP** in the upper-right corner of the topology to scan nearby APs that do not belong to the current network and are not connected to a network cable.

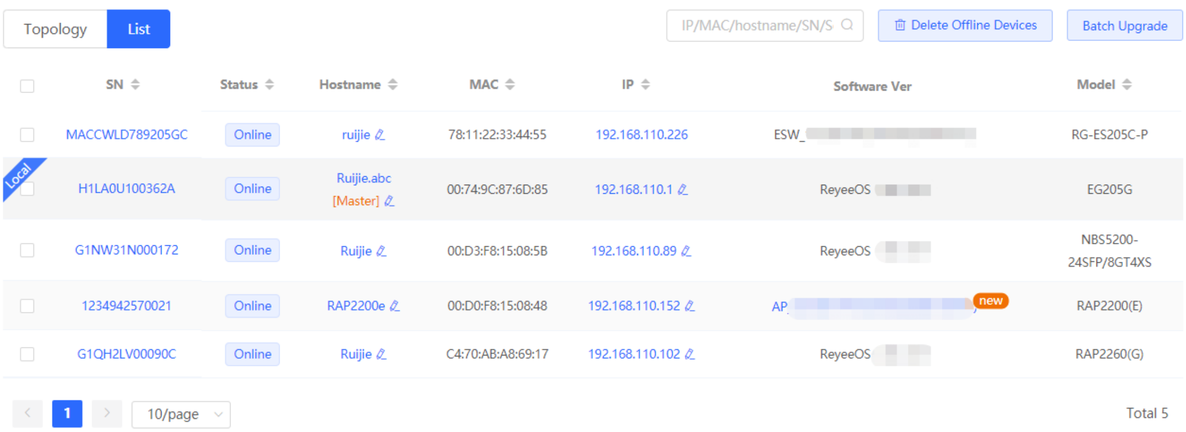


(2) Select the target AP to add it to the current network. You do not need to enter the password if the device to add is new. If the device has a password, enter the management password of the device.

10.4 Managing Networking Devices

On the **Overview** page, click **List** in the upper-left corner of the topology or click **Devices** in the menu bar to switch to the device list view. Then, you can view all the device information in the current networking. Users only need to log in to one device in the network to configure and manage devices in the entire network.





Topology | List

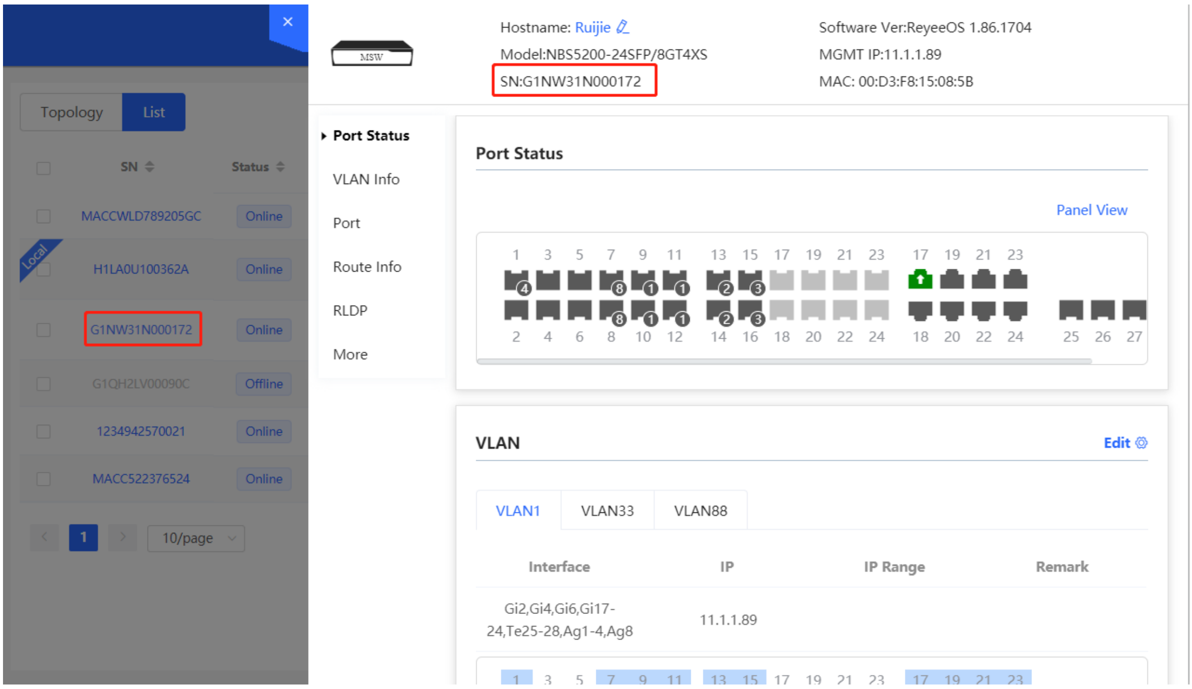
IP/MAC/hostname/SN/S

Delete Offline Devices | Batch Upgrade

SN	Status	Hostname	MAC	IP	Software Ver	Model
MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS	EG205G
G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	192.168.110.89	ReyeeOS	NBS5200-24SFP/8GT4XS
1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152	AP new	RAP2200(E)
G1QH2LV00090C	Online	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	ReyeeOS	RAP2260(G)

1 | 10/page | Total 5

- Click the device **SN** to configure the specified device separately.



Hostname: Ruijie

Model:NBS5200-24SFP/8GT4XS

SN:G1NW31N000172

Software Ver:ReyeeOS 1.86.1704

MGMT IP:11.1.1.89

MAC: 00:D3:F8:15:08:5B

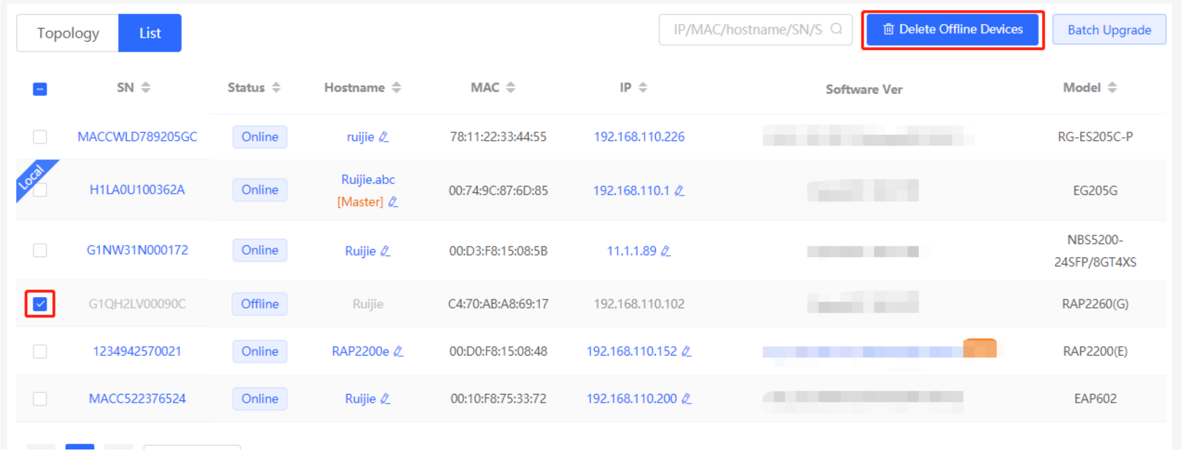
Port Status

VLAN

VLAN1 | VLAN33 | VLAN88

Interface	IP	IP Range	Remark
Gi2,Gi4,Gi6,Gi17-24,Te25-28,Ag1-4,Ag8	11.1.1.89		

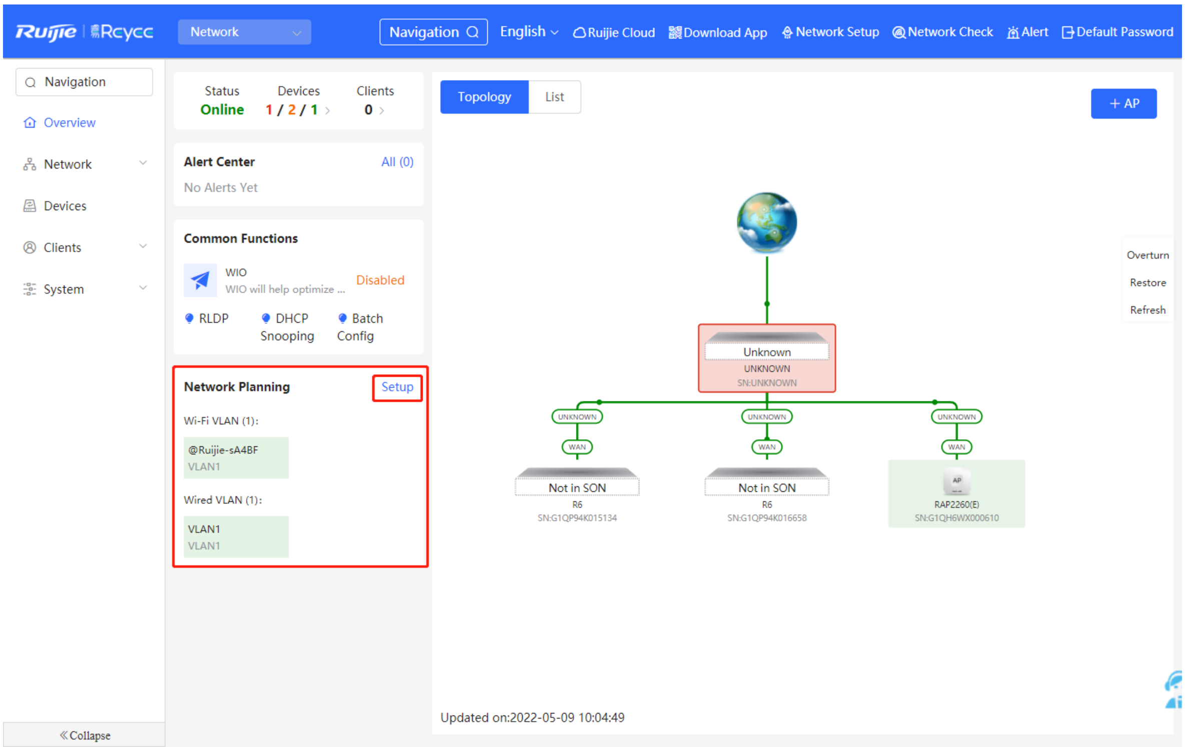
- Check offline devices and click **Delete Offline Devices** to remove them from the list and networking topology.



☐	SN	Status	Hostname	MAC	IP	Software Ver	Model
☐	MACCWLD789205GC	Online	ruijie	78:11:22:33:44:55	192.168.110.226	[redacted]	RG-ES205C-P
☐	H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	[redacted]	EG205G
☐	G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	11.1.1.89	[redacted]	NBS5200-24SFP/8GT4XS
☑	G1QH2LV00090C	Offline	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	[redacted]	RAP2260(G)
☐	1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152	[redacted]	RAP2200(E)
☐	MACC522376524	Online	Ruijie	00:10:F8:75:33:72	192.168.110.200	[redacted]	EAP602

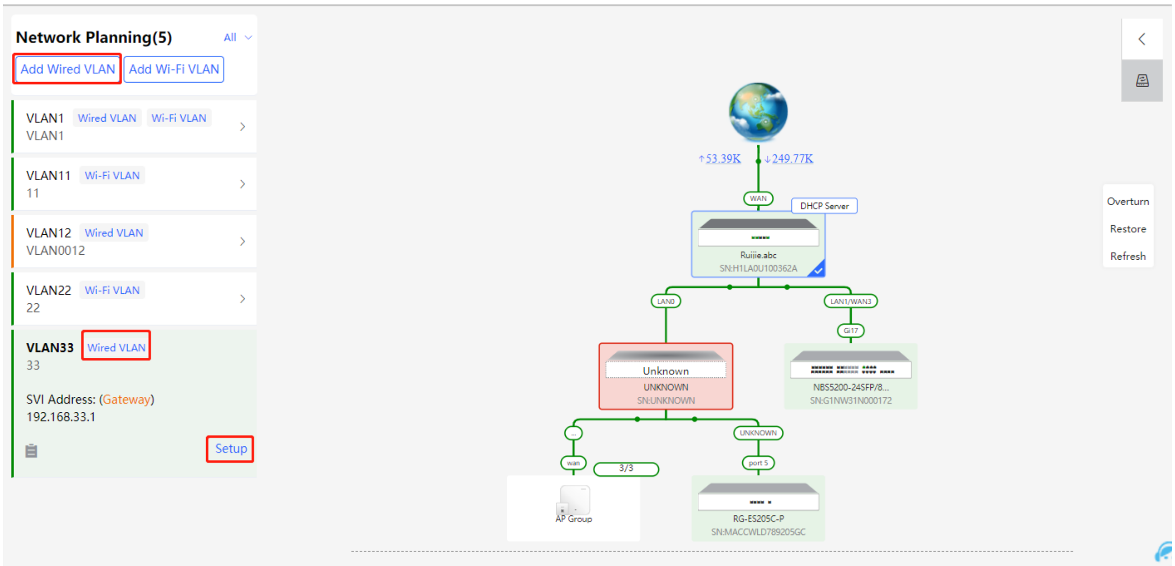
10.5 Configuring the Service Network

The wireless and wired network configurations of the current network are displayed in the lower-left of the **Overview** page. Click **Setup** to switch to the service network configuration page (or click **Network** > **Network Planning**).

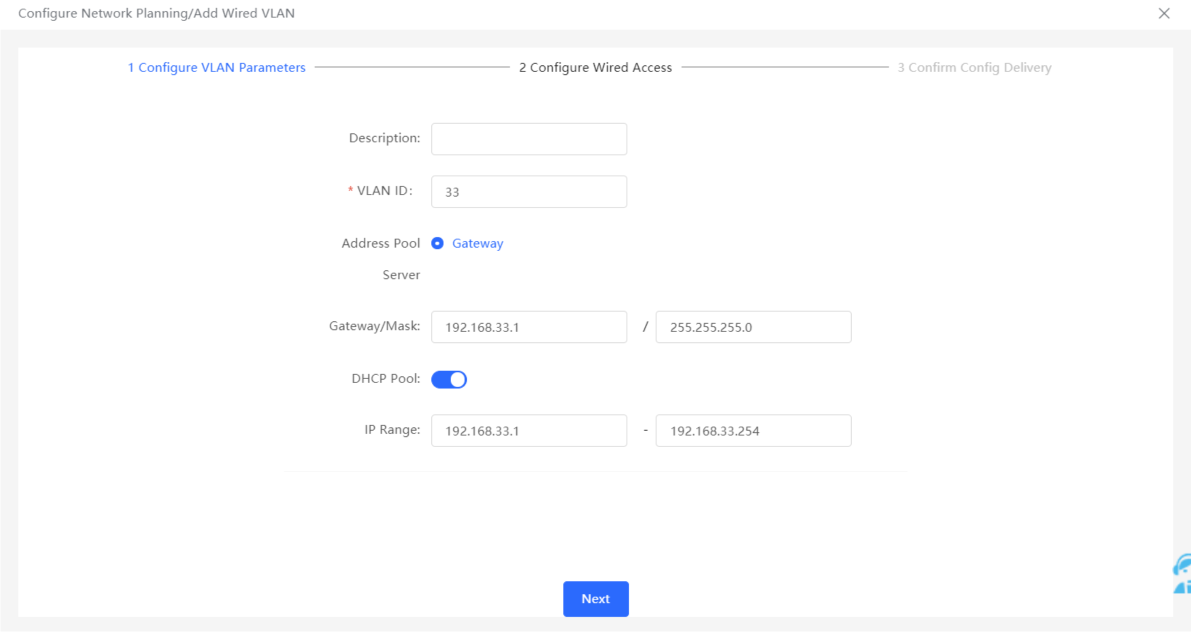


10.5.1 Configuring the Wired Network

(1) Click **Add Wired VLAN** to add wired network configuration, or select an existing wired VLAN and click **Setup** to modify its configuration.



(2) Configure a VLAN for wired access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. A switch or gateway device can be selected as the address pool server. After setting the service parameters, click **Next**.



Configure Network Planning/Add Wired VLAN

1 Configure VLAN Parameters — 2 Configure Wired Access — 3 Confirm Config Delivery

Description:

* VLAN ID: 33

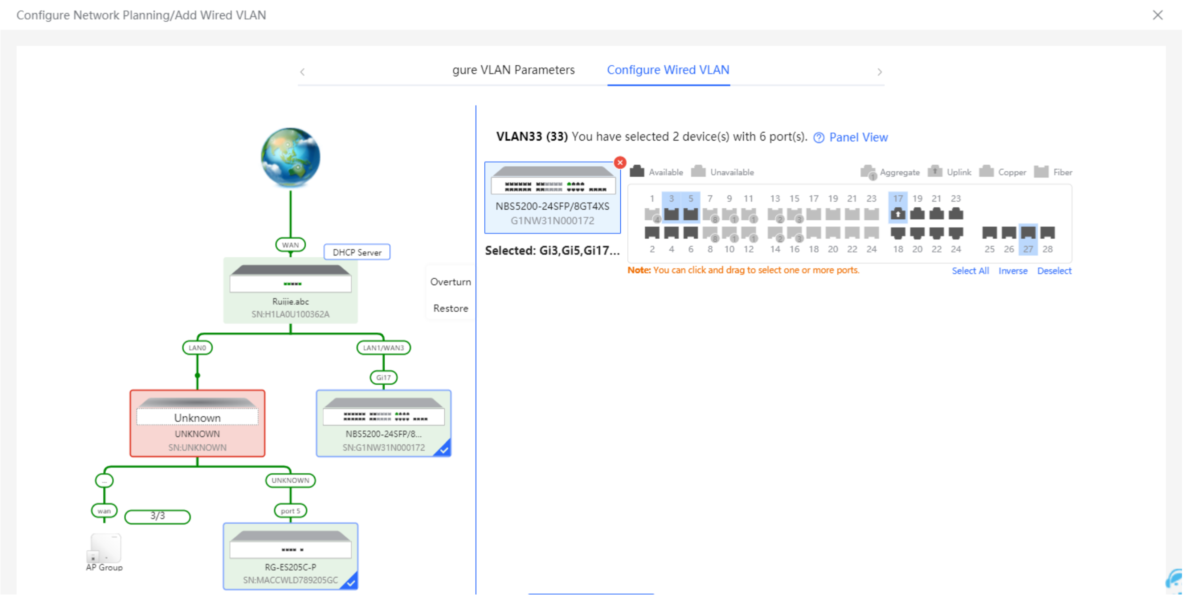
Address Pool Server: ● Gateway

Gateway/Mask: 192.168.33.1 / 255.255.255.0

DHCP Pool: (on)

IP Range: 192.168.33.1 - 192.168.33.254

(3) Select the switch to configure in the topology, select the switch ports added to this VLAN, and click **Next**.

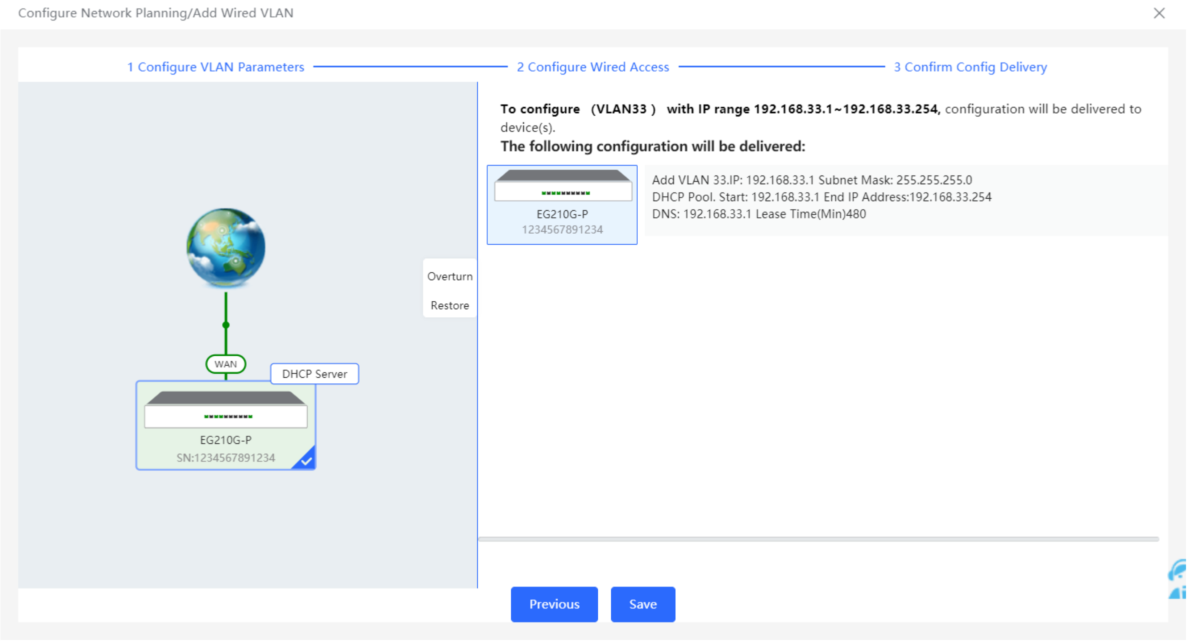


VLAN33 (33) You have selected 2 device(s) with 6 port(s).

Selected: Gi3,Gi5,Gi17...

Note: You can click and drag to select one or more ports.

(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.



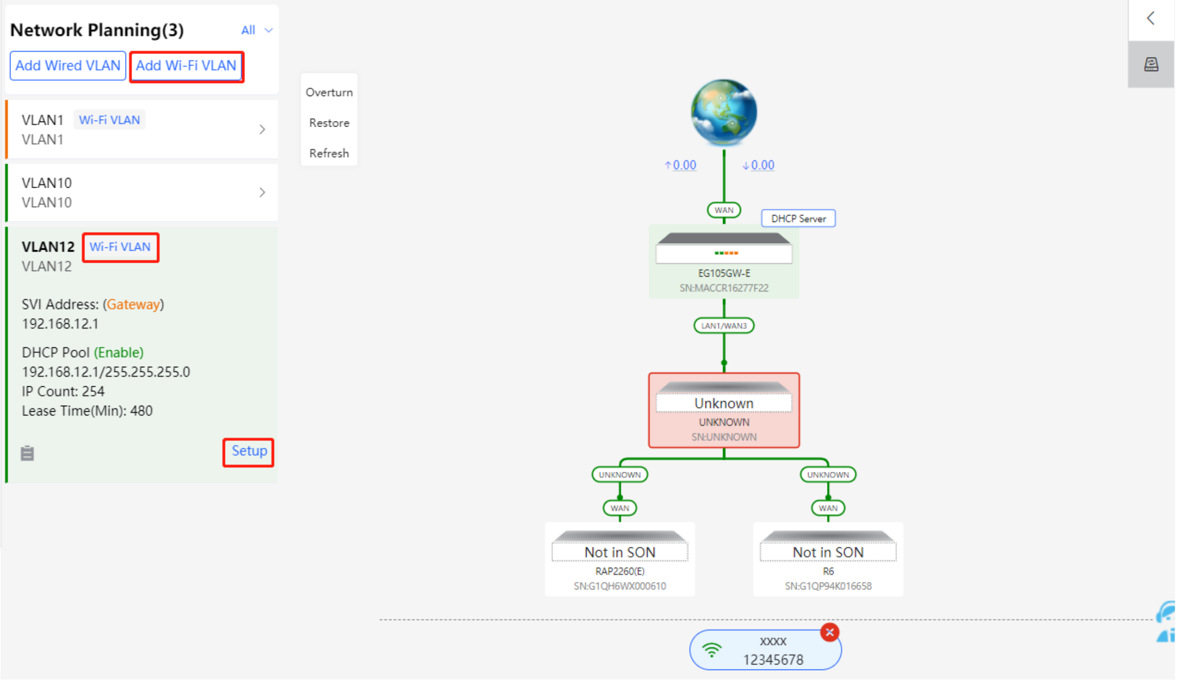
To configure (VLAN33) with IP range 192.168.33.1~192.168.33.254, configuration will be delivered to device(s).

The following configuration will be delivered:

Add VLAN 33.IP: 192.168.33.1 Subnet Mask: 255.255.255.0
DHCP Pool. Start: 192.168.33.1 End IP Address:192.168.33.254
DNS: 192.168.33.1 Lease Time(Min)480

10.5.2 Configuring the Wireless Network

(1) Click **Add Wi-Fi VLAN** to add wireless network configuration, or select an existing Wi-Fi VLAN and click **Setup** to modify its configuration.



Network Planning(3) All

Add Wired VLAN | Add Wi-Fi VLAN

VLAN1 Wi-Fi VLAN
VLAN1

VLAN10
VLAN10

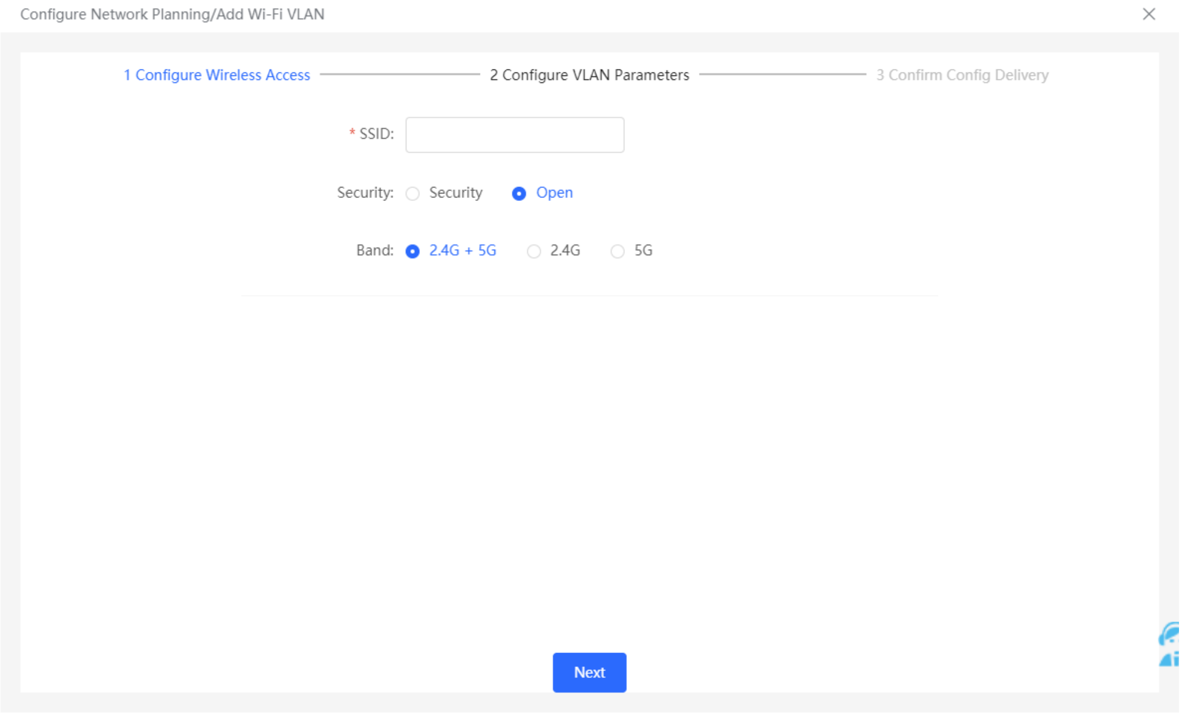
VLAN12 Wi-Fi VLAN
VLAN12

SVI Address: (Gateway)
192.168.12.1

DHCP Pool (Enable)
192.168.12.1/255.255.255.0
IP Count: 254
Lease Time(Min): 480

Setup

(2) Set the Wi-Fi name, Wi-Fi password, and applicable bands. Click **Next**.



Configure Network Planning/Add Wi-Fi VLAN

1 Configure Wireless Access — 2 Configure VLAN Parameters — 3 Confirm Config Delivery

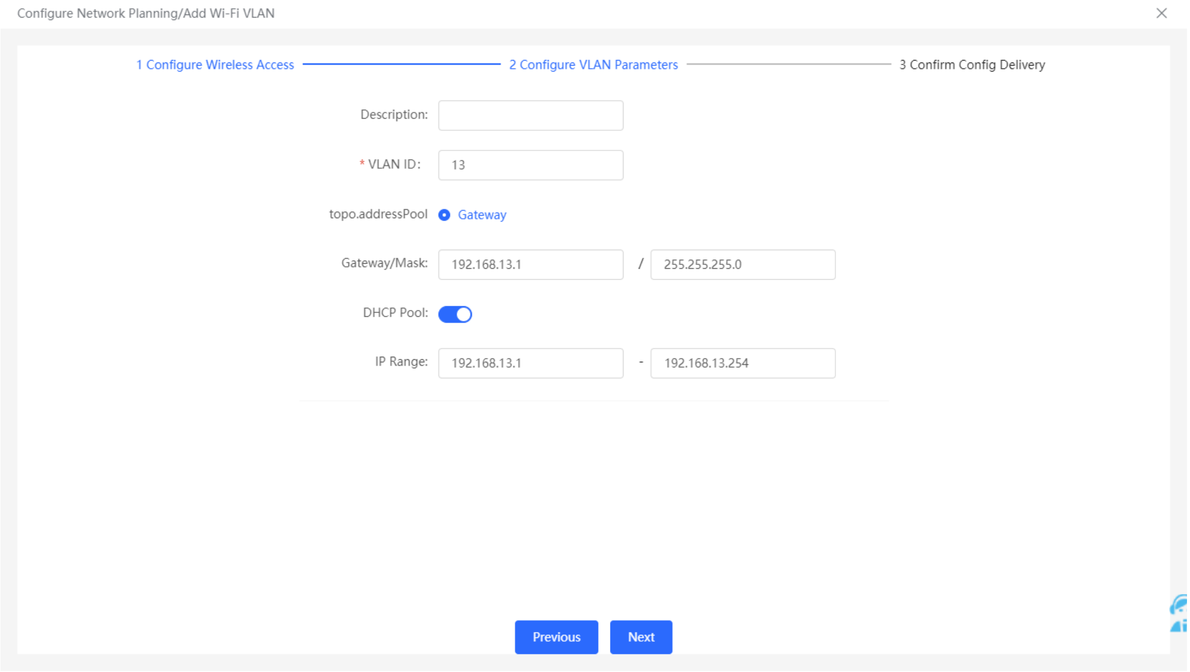
* SSID:

Security: ○ Security ● Open

Band: ● 2.4G + 5G ○ 2.4G ○ 5G

Next

(3) Configure a VLAN for wireless access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. A switch or gateway device can be selected as the address pool server. After setting the service parameters, click **Next**.


Configure Network Planning/Add Wi-Fi VLAN

1 Configure Wireless Access
2 Configure VLAN Parameters
3 Confirm Config Delivery

Description:

* VLAN ID: 13

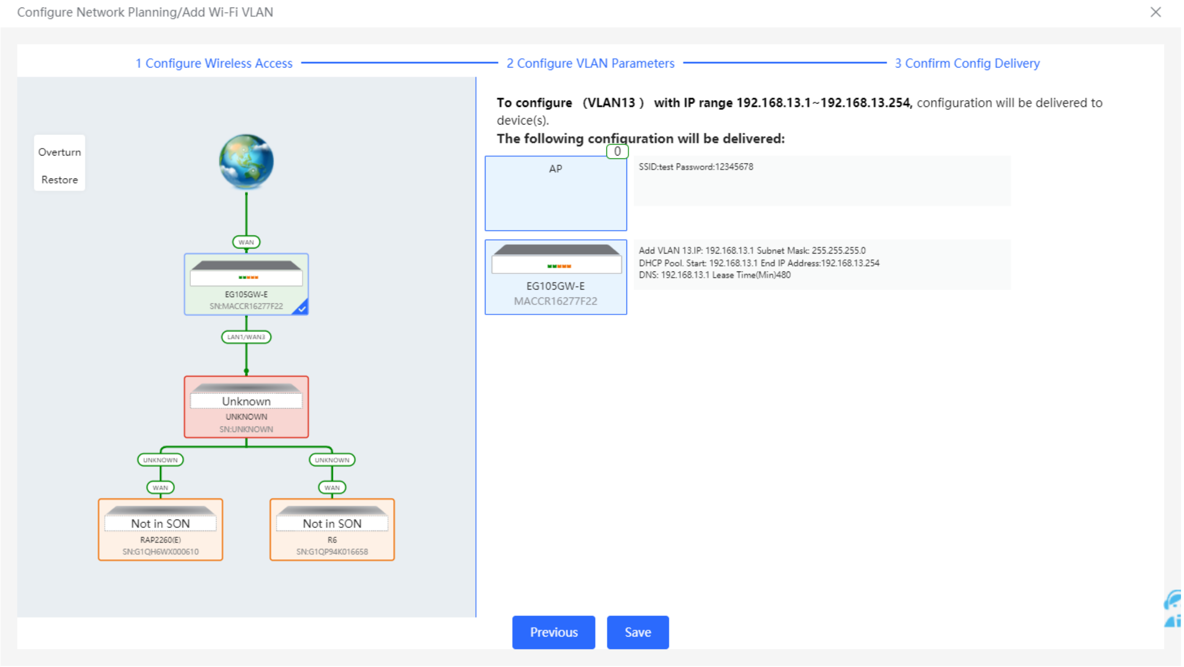
topo.addressPool ● Gateway

Gateway/Mask: 192.168.13.1 / 255.255.255.0

DHCP Pool: ●

IP Range: 192.168.13.1 - 192.168.13.254

(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.


Configure Network Planning/Add Wi-Fi VLAN

To configure (VLAN13) with IP range 192.168.13.1~192.168.13.254, configuration will be delivered to device(s).

The following configuration will be delivered:

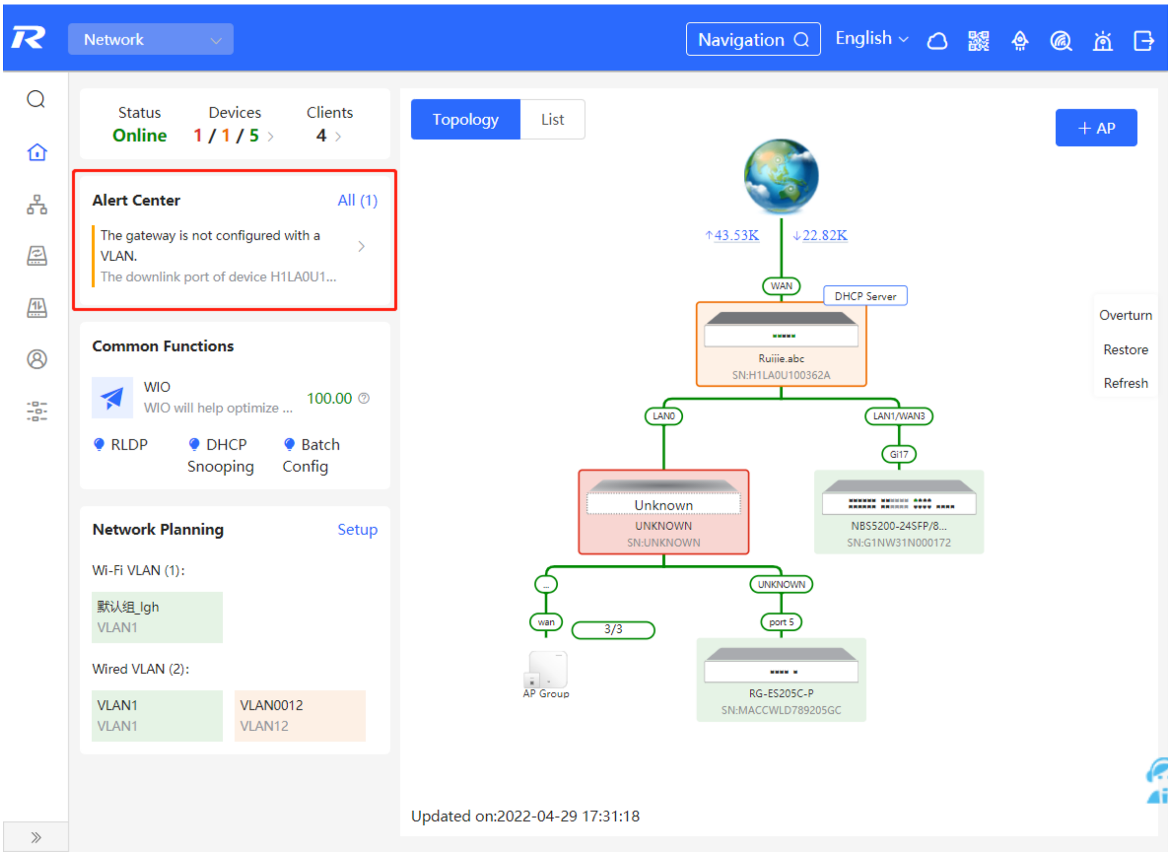
AP 0: SSID:test Password:12345678

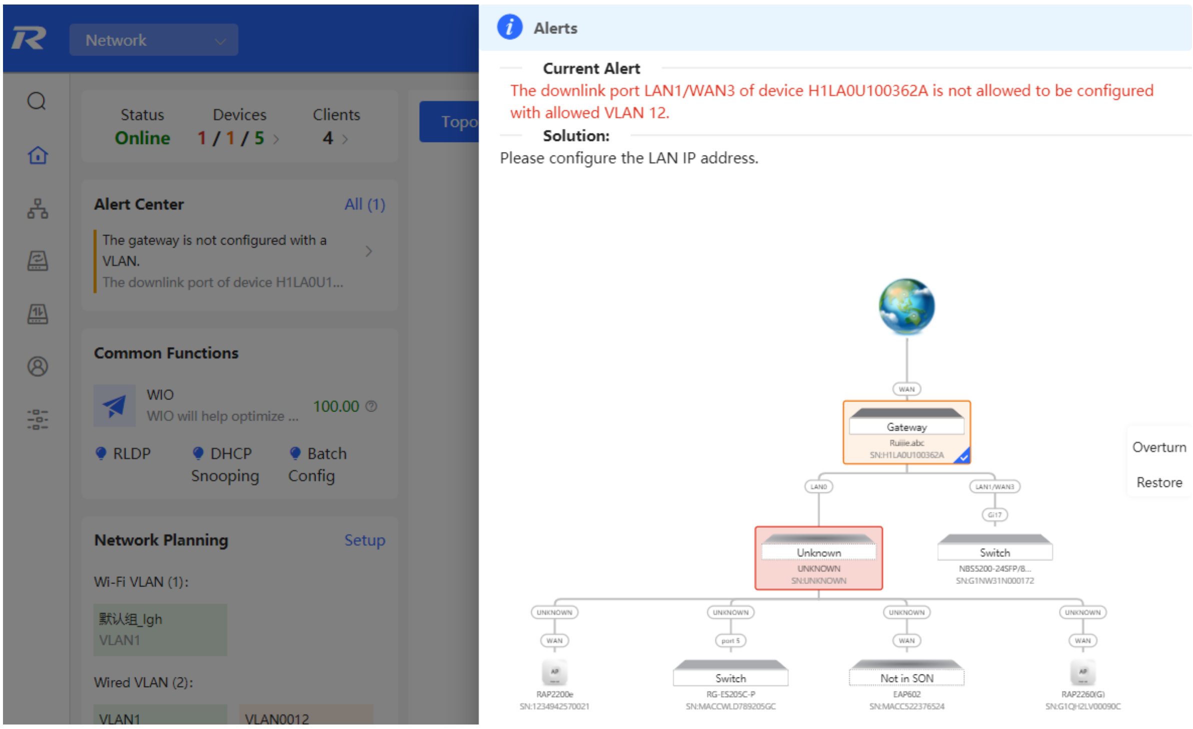
EG105GW-E MACCR16277F22:
Add VLAN 13.IP: 192.168.13.1 Subnet Mask: 255.255.255.0
DHCP Pool. Start: 192.168.13.1 End IP Address:192.168.13.254
DNS: 192.168.13.1 Lease Time(Min)480

10.6 Processing Alerts

Choose **Network** > **Overview**.

If a network exception occurs, alert message on this exception and the corresponding solution are displayed on the **Overview** page. Click the alert message in the **Alert Center** section to view the faulty device, problem details, and its solution. Troubleshoot and process the alert according to the solution.





Current Alert

The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12.

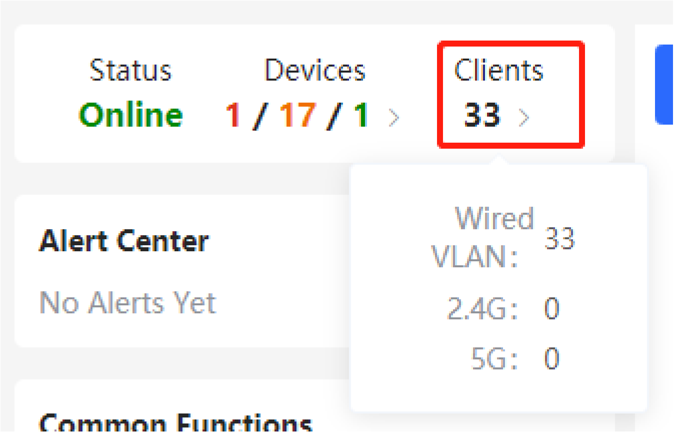
Solution:

Please configure the LAN IP address.

10.7 Viewing Online Clients

The **Clients** in the upper-left corner of the **Overview** page displays the total number of online clients in the current network; moving the cursor to the number of users will display the number of current wired users, wireless users in the 2.4GHz band, and wireless users in the 5GHz band.

Click to switch to the online clients page (or click **Clients** > **Online Clients**).



Status: Online

Devices: 1 / 17 / 1

Clients: 33

Wired VLAN: 33

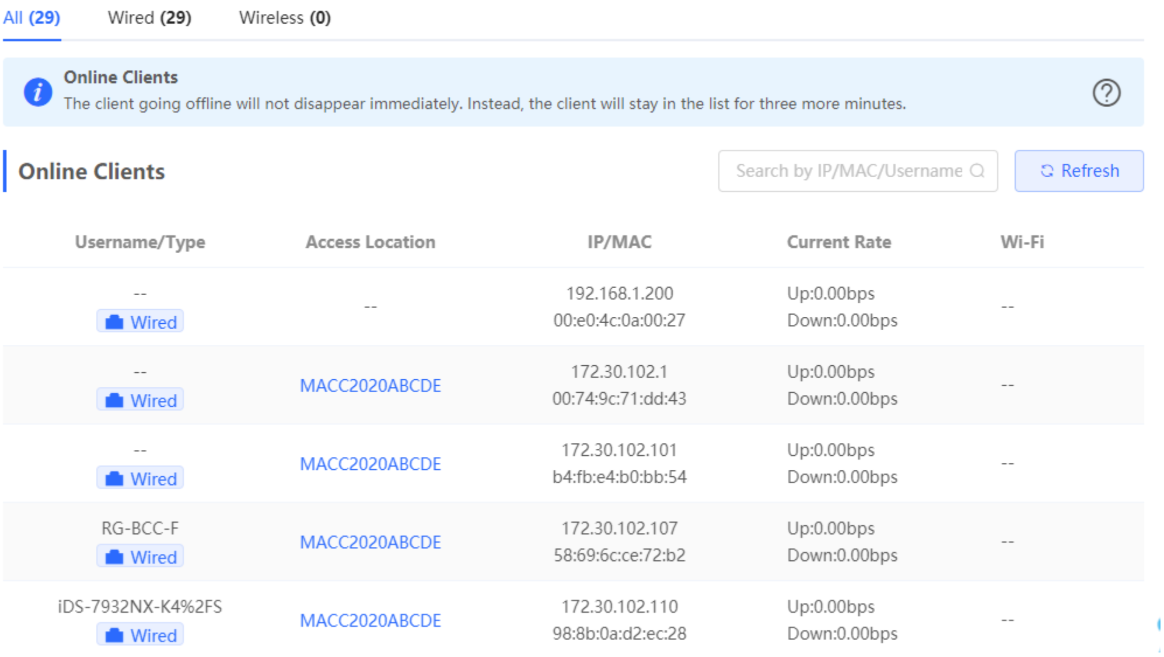
2.4G: 0

5G: 0

Alert Center

No Alerts Yet

Common Functions



All (29) Wired (29) Wireless (0)

Online Clients

The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.

Online Clients

Username/Type	Access Location	IP/MAC	Current Rate	Wi-Fi
-- Wired	--	192.168.1.200 00:e0:4c:0a:00:27	Up:0.00bps Down:0.00bps	--
-- Wired	MACC2020ABCDE	172.30.102.1 00:74:9c:71:dd:43	Up:0.00bps Down:0.00bps	--
-- Wired	MACC2020ABCDE	172.30.102.101 b4:fb:e4:b0:bb:54	Up:0.00bps Down:0.00bps	--
RG-BCC-F Wired	MACC2020ABCDE	172.30.102.107 58:69:6c:ce:72:b2	Up:0.00bps Down:0.00bps	--
iDS-7932NX-K4%2FS Wired	MACC2020ABCDE	172.30.102.110 98:8b:0a:d2:ec:28	Up:0.00bps Down:0.00bps	--

Table 10-1 Description of Online Client Information

Field	Description
Username/Type	Indicate the name and access type of the client. The access type can be wireless or wired.
Access Location	Indicate the SN of the device that the user accesses to. You can click it to view the access port during wired access.
IP/MAC	The IP address and the MAC address of the client.
Current Rate	Indicate the uplink and downlink data transmission rates of the client.
Wi-Fi	Wireless network information associated with wireless clients, including channel, signal strength, online time, negotiation rate, etc.

10.8 Smart Device Network

Caution

Currently, the function is supported by RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series devices.

10.8.1 Overview

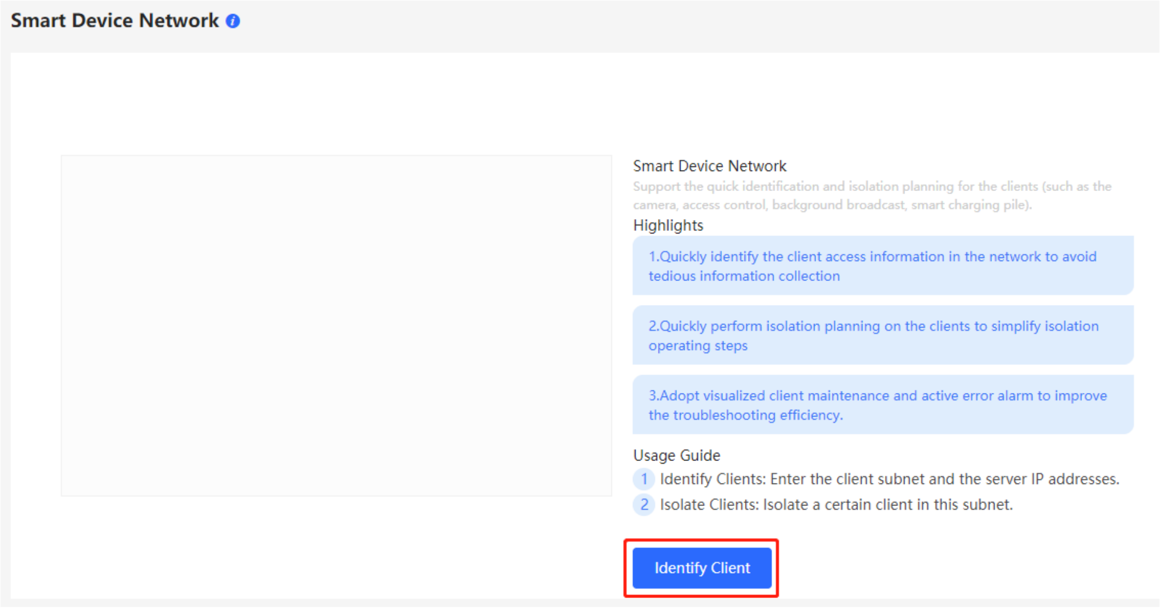
The smart device network is used to quickly plan and set up an isolation network for smart clients, so as to isolate the client network from the normal service network and other types of clients, and improve the stability of the network. The smart device network supports rapid identification of various types of clients (such as cameras, access control, background broadcasting, smart charging piles, etc.) and batch execution of isolation planning on clients. Compared with traditional client network planning and deployment steps, it eliminates the tedious process, collects information and simplifies the steps to set up client isolation.

After setting up the smart device network, the page visually displays client information, and actively alerts abnormality, which can effectively improve the efficiency of troubleshooting.

10.8.2 Procedure

Choose **Network** > **Clients** > **Smart Device Network**.

(1) Click **Identify Client**.



Smart Device Network

Support the quick identification and isolation planning for the clients (such as the camera, access control, background broadcast, smart charging pile).

Highlights

1.Quickly identify the client access information in the network to avoid tedious information collection

2.Quickly perform isolation planning on the clients to simplify isolation operating steps

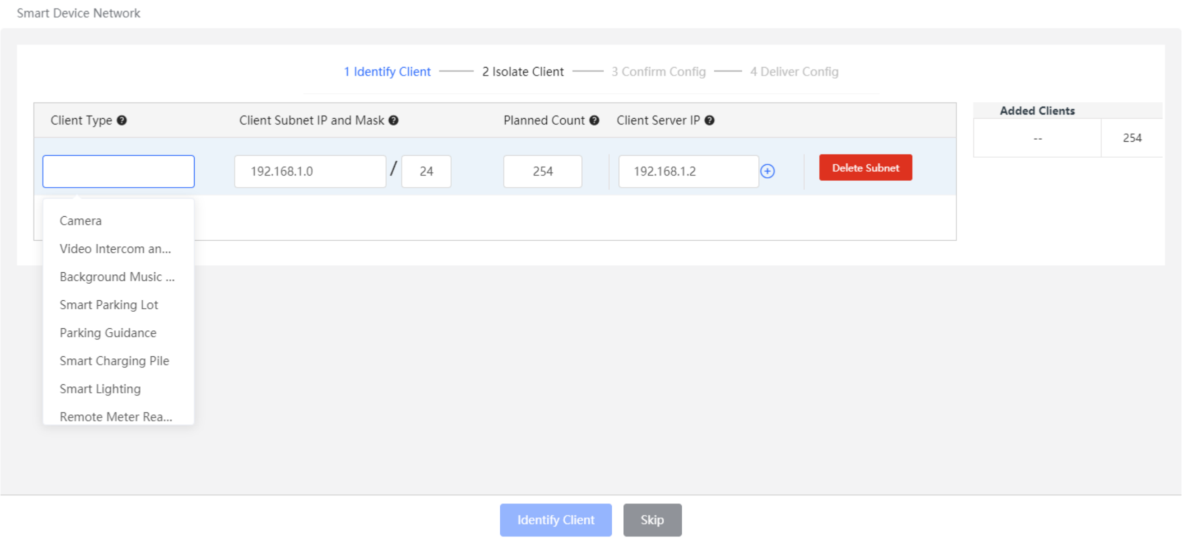
3.Adopt visualized client maintenance and active error alarm to improve the troubleshooting efficiency.

Usage Guide

1 Identify Clients: Enter the client subnet and the server IP addresses.

2 Isolate Clients: Isolate a certain client in this subnet.

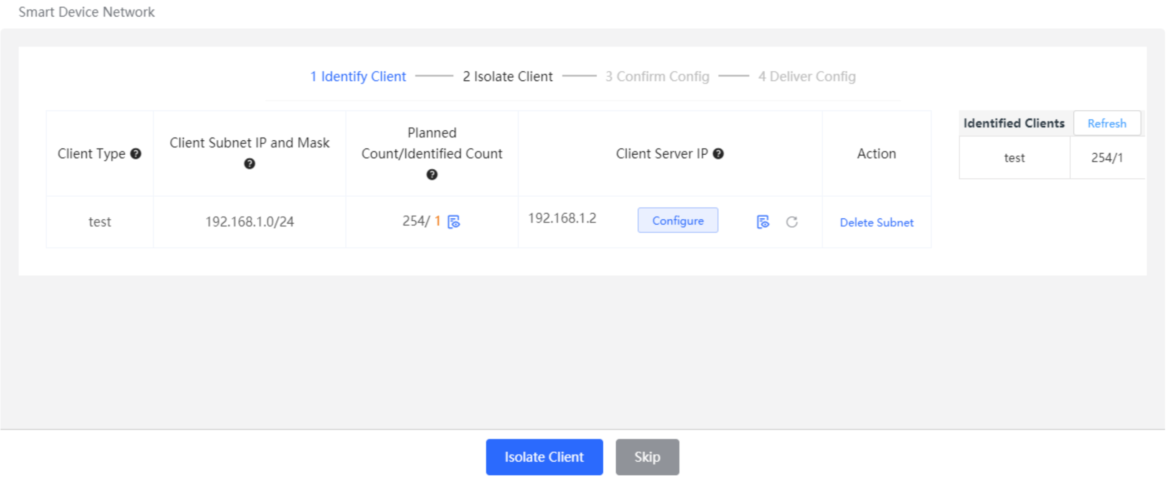
(2) Click **+Client Subnet**, enter the client type (which can be selected or customized in the drop-down box), the network segment of the client, the planned number and the corresponding server IP address to identify the client. Multi-type client network segments can be set. Click **Identify Client** after filling in.



Client Type	Client Subnet IP and Mask	Planned Count	Client Server IP
	192.168.1.0 / 24	254	192.168.1.2

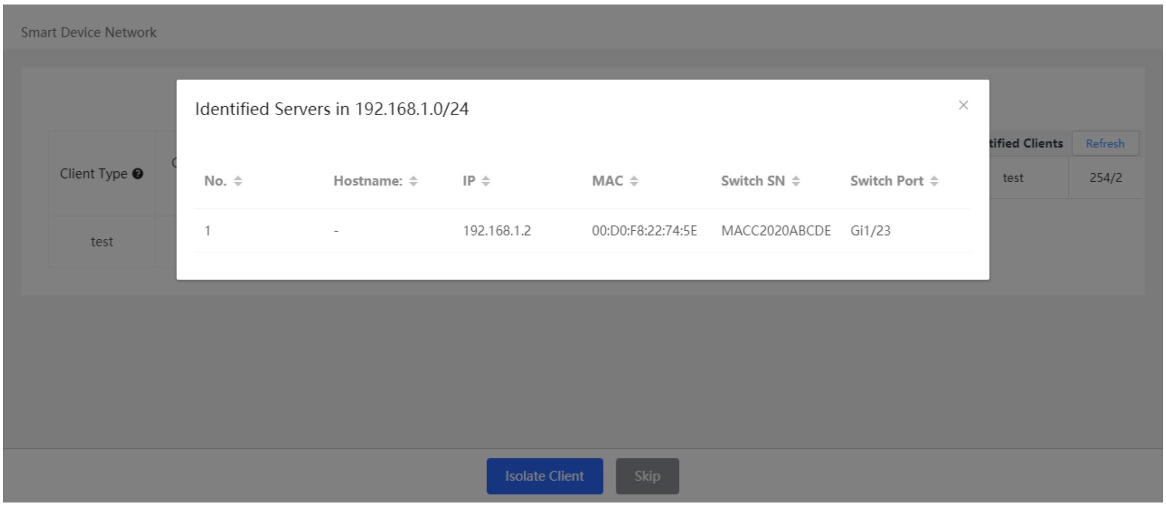
Added Clients	
--	254

(3) Display the identified client and client server information, including IP address, MAC address, SN number of the connected switch and connection port. Click to view the detailed information. If the connection information to the client server is not identified, you need to click **Configure** and fill in the relevant information manually. After confirming that the client device information is correct, click **Isolate Client**.



Client Type	Client Subnet IP and Mask	Planned Count/Identified Count	Client Server IP	Action
test	192.168.1.0/24	254/ 1	192.168.1.2	Delete Subnet

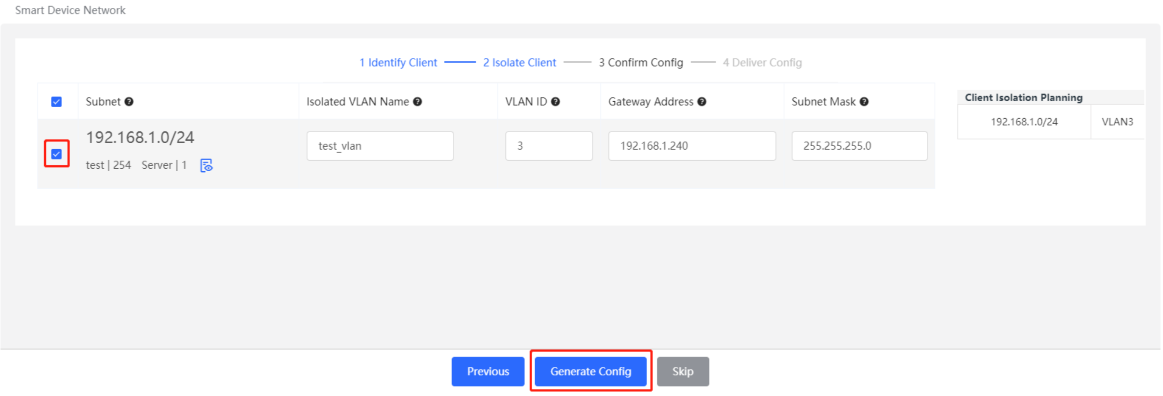
Identified Clients	
test	254/1



Identified Servers in 192.168.1.0/24

No.	Hostname:	IP	MAC	Switch SN	Switch Port
1	-	192.168.1.2	00:D0:F8:22:74:5E	MACC2020ABCDE	Gi1/23

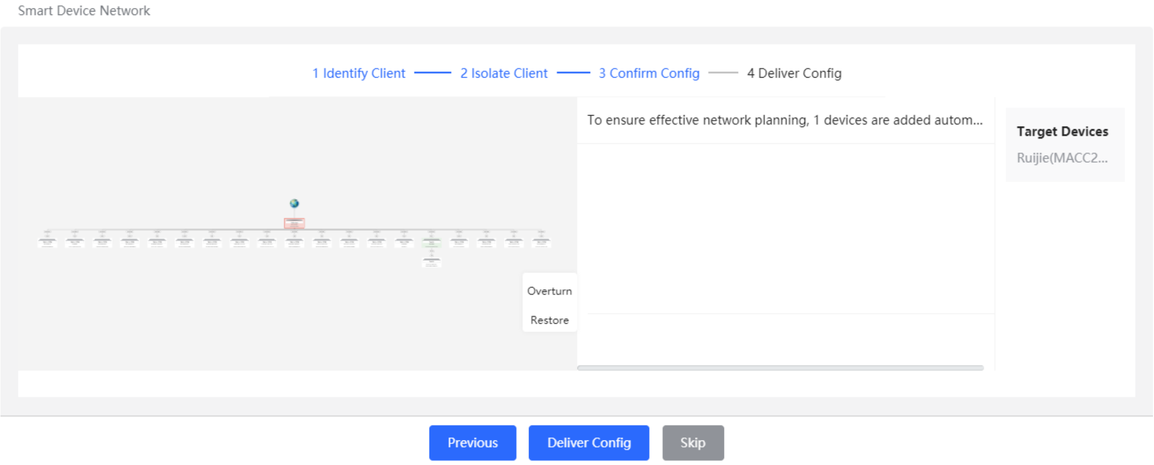
(4) Input the name of the VLAN, VLAN ID, gateway address, and subnet mask of the isolated client. Check the target network segment and click **Generate Config**.



☑	Subnet	Isolated VLAN Name	VLAN ID	Gateway Address	Subnet Mask
☑	192.168.1.0/24 test | 254 Server | 1	test_vlan	3	192.168.1.240	255.255.255.0

Client Isolation Planning	
192.168.1.0/24	VLAN3

(5) After confirming the configuration, click **Deliver Config**. If you need to modify it, you can click **Previous** to return to the setting page.

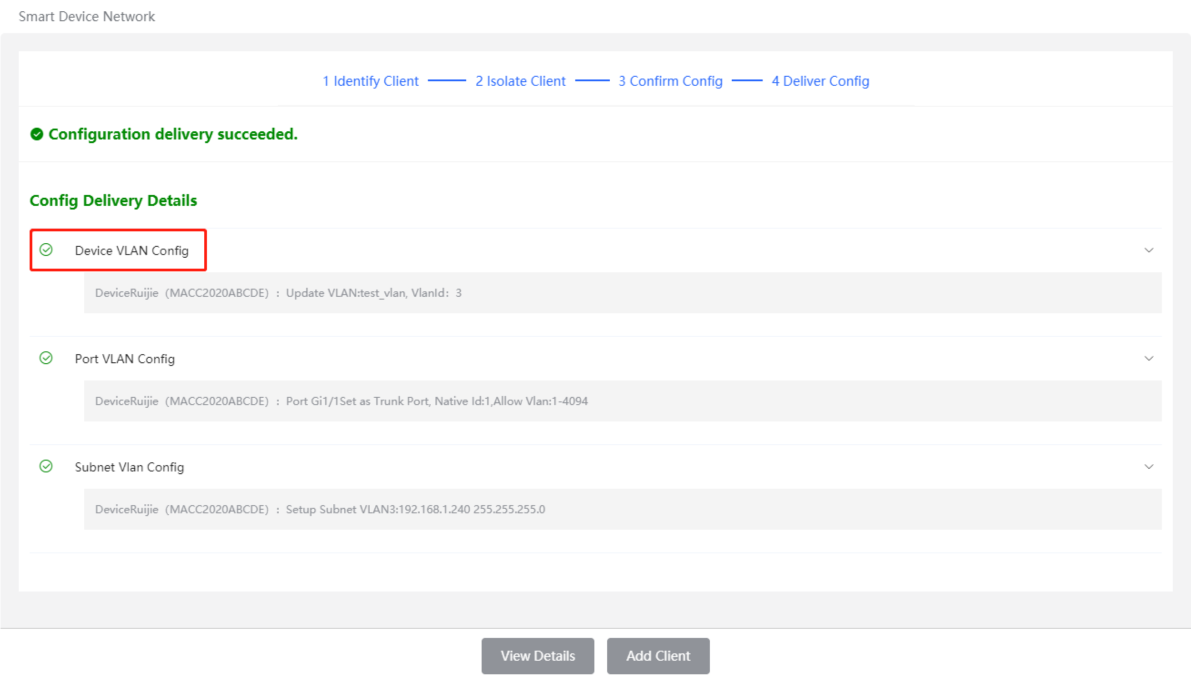


To ensure effective network planning, 1 devices are added autom...

Target Devices

Ruijie(MACC2...

(6) The page displays that the configuration has been delivered successfully, indicating that the settings have been completed. Click the configuration item to view the configuration delivery details. After the configuration is delivered, click **View Details** to switch to the page that displays monitoring information of the smart device network; click **Add Client** to continue setting the client network segment.



Smart Device Network

1 Identify Client —— 2 Isolate Client —— 3 Confirm Config —— 4 Deliver Config

Configuration delivery succeeded.

Config Delivery Details

Device VLAN Config

DeviceRuijie（MACC2020ABCDE）：Update VLAN:test_vlan, VlanId：3

Port VLAN Config

DeviceRuijie（MACC2020ABCDE）：Port Gi1/1Set as Trunk Port, Native Id:1,Allow Vlan:1-4094

Subnet Vlan Config

DeviceRuijie（MACC2020ABCDE）：Setup Subnet VLAN3:192.168.1.240 255.255.255.0

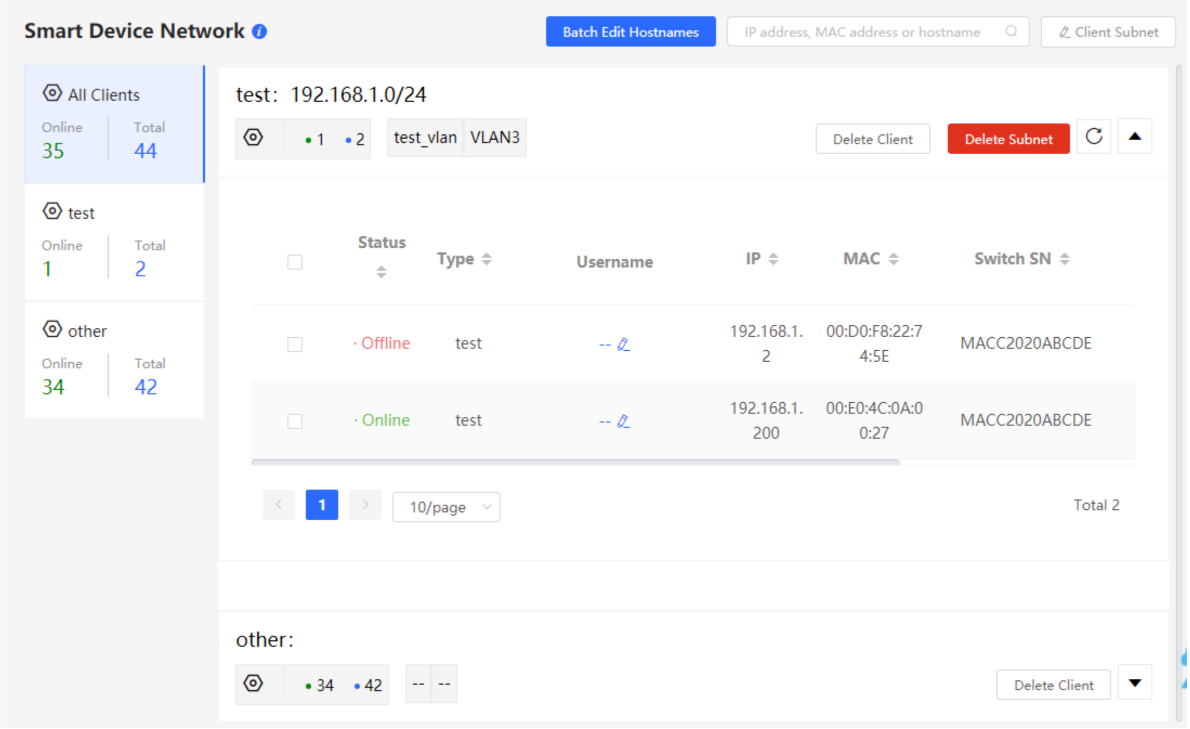
(7) After completing the smart device network settings, you can view the client monitoring information on the page, including client online status, connection information, device information, and online and offline time.

Select the client entry and click **Delete Client** to remove the specified client from the current network.

Click **Batch Edit Hostnames** to import a txt file containing client IP and client name (one line for each client, each line contains an IP and a name, and the IP and the name are separated by the Tab key), and modify the client names in batches.

Click **Client Subnet** to modify servers and isolate VLAN information, or add a new client network segment.

Click **Delete Subnet** to delete the corresponding smart device network configuration.



Smart Device Network

All Clients: Online 35, Total 44

test: Online 1, Total 2

other: Online 34, Total 42

test：192.168.1.0/24

• 1 • 2 test_vlan VLAN3

	Status	Type	Username	IP	MAC	Switch SN
□	· Offline	test	--	192.168.1.2	00:D0:F8:22:74:5E	MACC2020ABCDE
□	· Online	test	--	192.168.1.200	00:E0:4C:0A:00:27	MACC2020ABCDE

1 10/page Total 2

other：

• 34 • 42 -- --

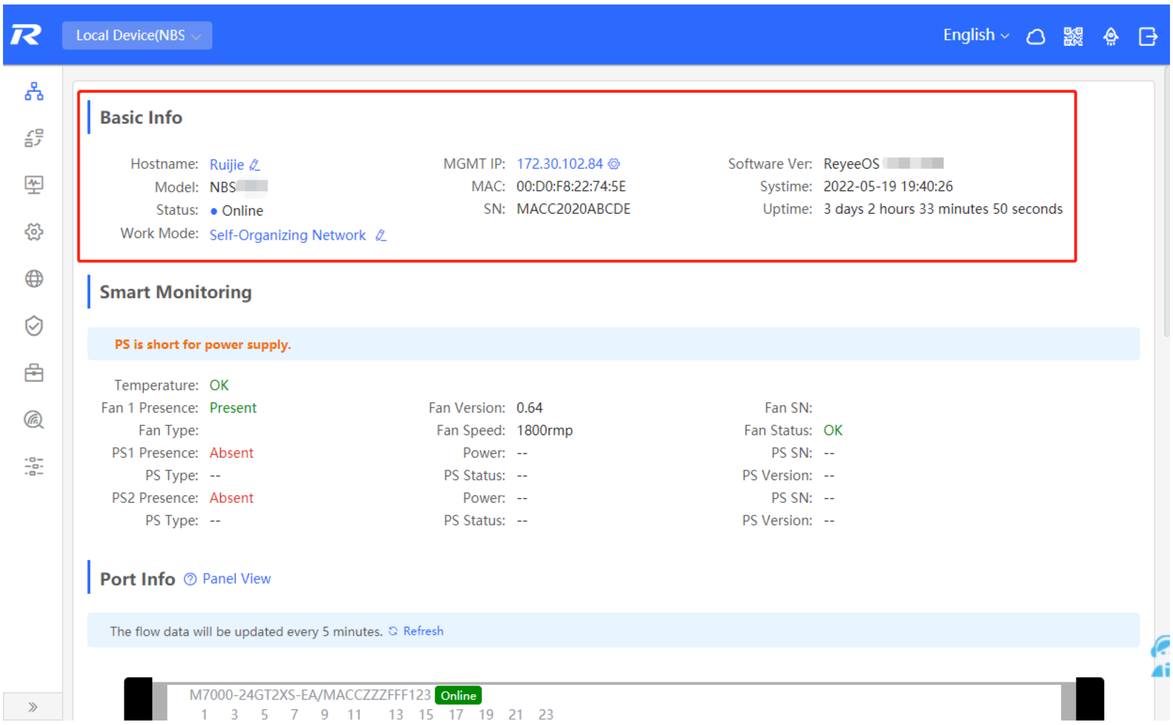
11 NBS Series Basic Management

11.1 Overviewing Switch Information

11.1.1 Basic information about the Device

Choose **Local Device** > **Home** > **Basic Info**.

Basic information includes device name, device model, SN number, software version, management IP, MAC address, networking status, system time, working mode, etc.



Basic Info

Hostname: Ruijie
Model: NBS[redacted]
Status: ● Online
Work Mode: Self-Organizing Network
MGMT IP: 172.30.102.84
MAC: 00:D0:F8:22:74:5E
SN: MACC2020ABCDE
Software Ver: ReyeeOS [redacted]
Systime: 2022-05-19 19:40:26
Uptime: 3 days 2 hours 33 minutes 50 seconds

Smart Monitoring

PS is short for power supply.

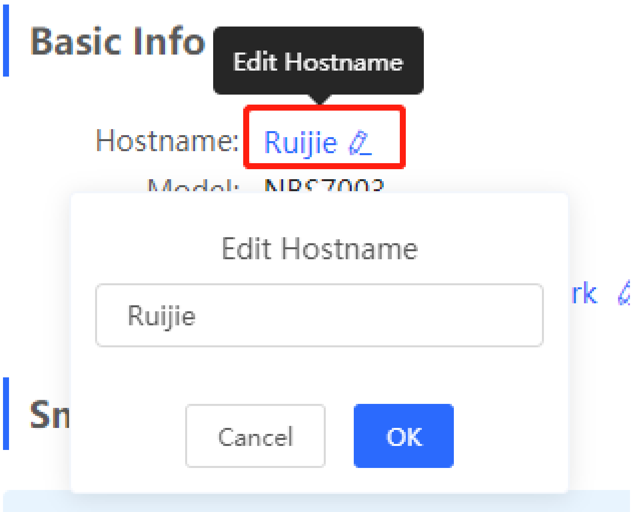
Temperature: OK
Fan 1 Presence: Present
Fan Type:
PS1 Presence: Absent
PS Type: --
PS2 Presence: Absent
PS Type: --
Fan Version: 0.64
Fan Speed: 1800rmp
Power: --
PS Status: --
Power: --
PS Status: --
Fan SN:
Fan Status: OK
PS SN: --
PS Version: --
PS SN: --
PS Version: --

Port Info Panel View

The flow data will be updated every 5 minutes. Refresh

1. **Setting the device name**

Click the device name to modify the device name in order to distinguish between different devices.

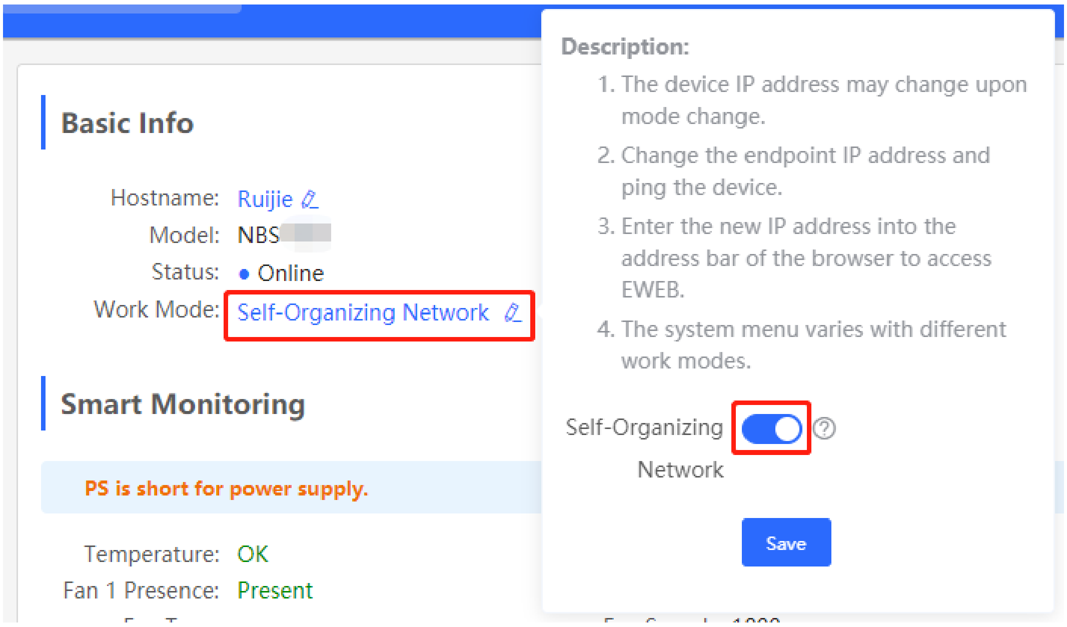


Edit Hostname

Ruijie

2. **Switching the Work Mode**

Click the current work mode to change the work mode.



Basic Info

Hostname: Ruijie

Model: NBS[redacted]

Status: ● Online

Work Mode: Self-Organizing Network

Smart Monitoring

PS is short for power supply.

Temperature: OK

Fan 1 Presence: Present

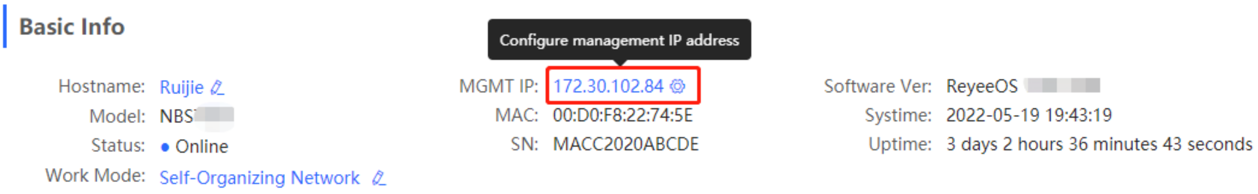
Description:

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access EWEB.
4. The system menu varies with different work modes.

Self-Organizing Network: ●

3. **Setting MGMT IP**

Click current management IP address to jump to the management IP configuration page. For more information, see 12.6 .



Basic Info

Hostname: Ruijie

Model: NBS[redacted]

Status: ● Online

Work Mode: Self-Organizing Network

MGMT IP: 172.30.102.84

MAC: 00:D0:F8:22:74:5E

SN: MACC2020ABCDE

Software Ver: ReyeeOS [redacted]

Systime: 2022-05-19 19:43:19

Uptime: 3 days 2 hours 36 minutes 43 seconds

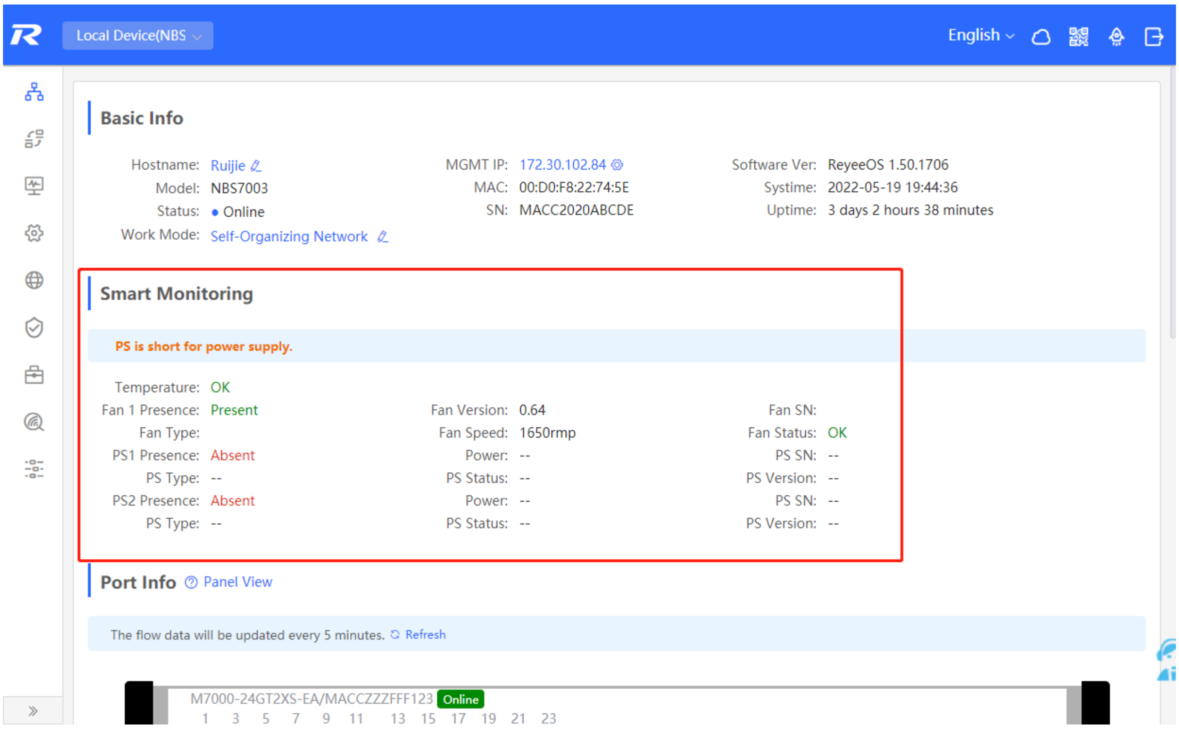
11.1.2 Hardware Monitor Information

Caution

Only RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series devices support displaying this type of information.

Choose **Local Device** > **Home** > **Smart Monitoring**.

Display the current hardware operating status of the device, such as the device temperature and power supply status, etc.



Basic Info

Hostname:	Ruijie	MGMT IP:	172.30.102.84	Software Ver:	ReyeeOS 1.50.1706
Model:	NBS7003	MAC:	00:D0:F8:22:74:5E	Systime:	2022-05-19 19:44:36
Status:	● Online	SN:	MACC2020ABCDE	Uptime:	3 days 2 hours 38 minutes
Work Mode:	Self-Organizing Network				

Smart Monitoring

PS is short for power supply.

Temperature:	OK				
Fan 1 Presence:	Present	Fan Version:	0.64	Fan SN:	
Fan Type:		Fan Speed:	1650rmp	Fan Status:	OK
PS1 Presence:	Absent	Power:	--	PS SN:	--
PS Type:	--	PS Status:	--	PS Version:	--
PS2 Presence:	Absent	Power:	--	PS SN:	--
PS Type:	--	PS Status:	--	PS Version:	--

Port Info Panel View

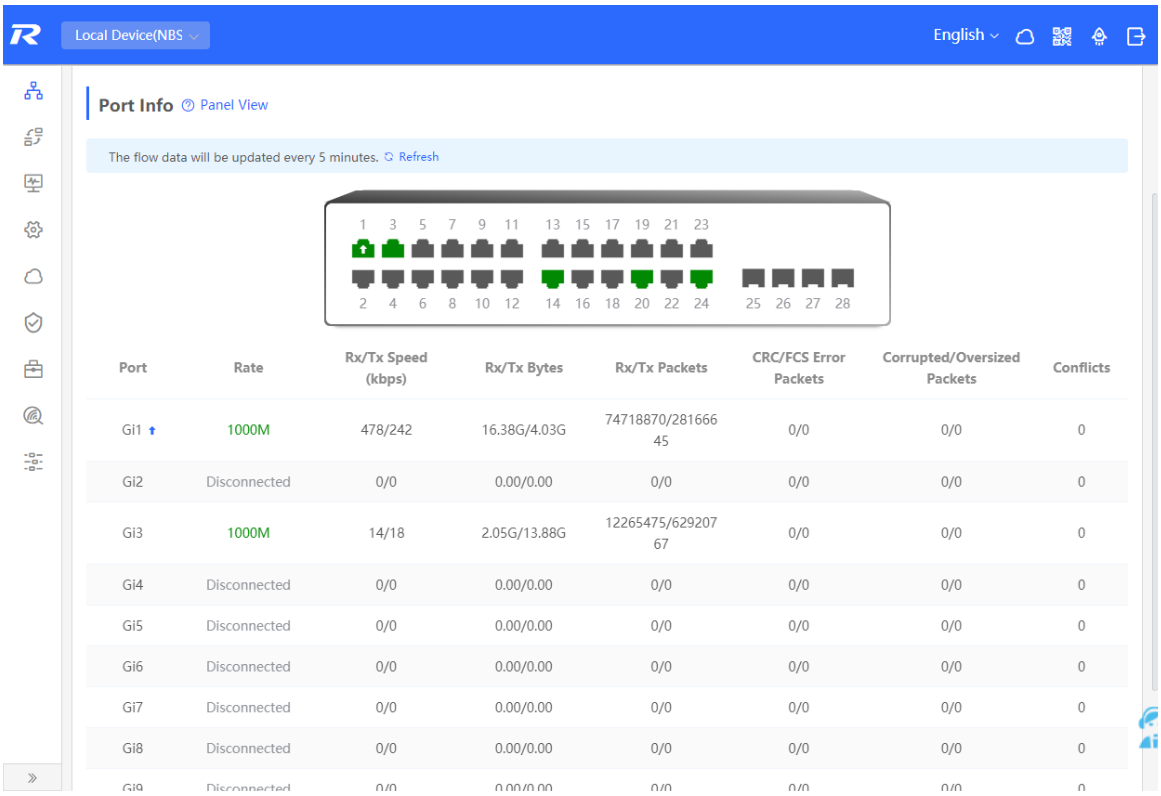
The flow data will be updated every 5 minutes. Refresh

M7000-24GT2XS-EA/MACCZZZFFF123 Online

11.1.3 Port Info

Choose **Local Device** > **Home** > **Port Info**.

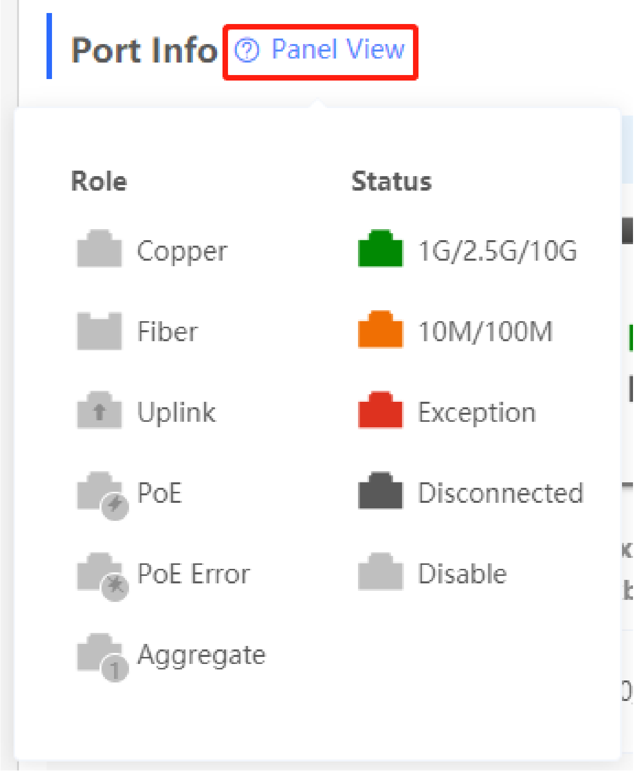
- The port info page displays the details of all ports currently on the switch. Click **Panel View** to view the port roles and statuses corresponding to port icons of different colors or shapes.



Port Info Panel View

The flow data will be updated every 5 minutes. Refresh

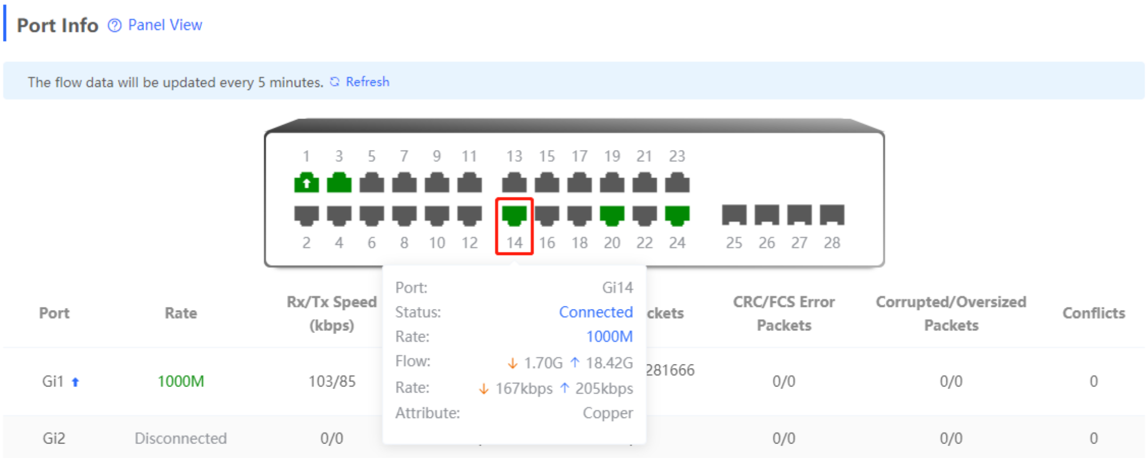
Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1 ↑	1000M	478/242	16.38G/4.03G	74718870/28166645	0/0	0/0	0
Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi3	1000M	14/18	2.05G/13.88G	12265475/62920767	0/0	0/0	0
Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi7	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi8	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi9	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0



Port Info ⓘ Panel View

Role	Status
Copper	1G/2.5G/10G
Fiber	10M/100M
Uplink	Exception
PoE	Disconnected
PoE Error	Disable
Aggregate	

- Move the cursor to the icon of a port (for example, Gi14) on the port panel, and more information about the port will be displayed, including the port ID, port status, port rate, uplink and downlink traffic, transmission rate, and optical/electrical attribute of the port.



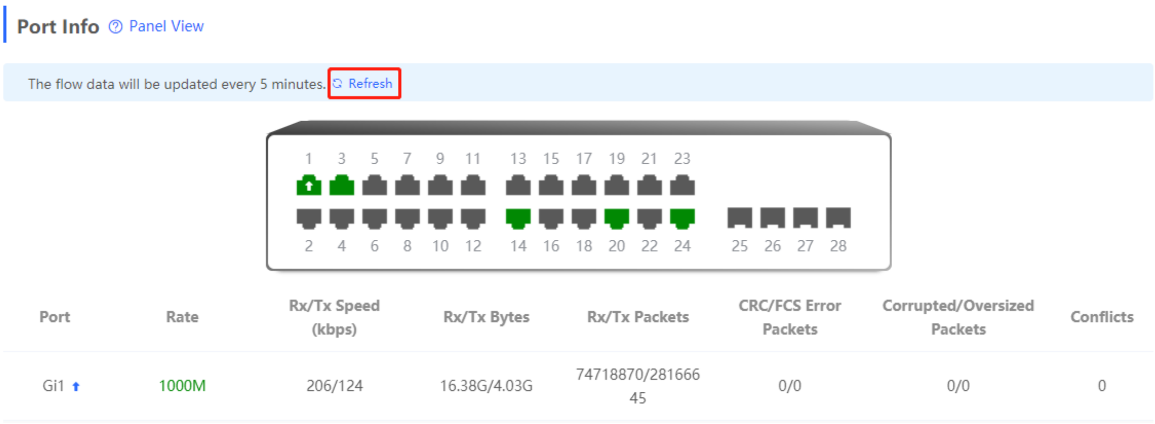
Port Info ⓘ Panel View

The flow data will be updated every 5 minutes. Refresh

Port: Gi14
Status: Connected
Rate: 1000M
Flow: ↓ 1.70G ↑ 18.42G
Rate: ↓ 167kbps ↑ 205kbps
Attribute: Copper

Port	Rate	Rx/Tx Speed (kbps)	ckets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1 ↑	1000M	103/85	281666	0/0	0/0	0
Gi2	Disconnected	0/0		0/0	0/0	0

- Traffic data is automatically updated every five minutes. You can click **Refresh** above the port panel to obtain the latest port traffic and status information simultaneously.



Port Info Panel View

The flow data will be updated every 5 minutes. Refresh

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1 ↑	1000M	206/124	16.38G/4.03G	74718870/28166645	0/0	0/0	0

11.2 Port Flow Statistics

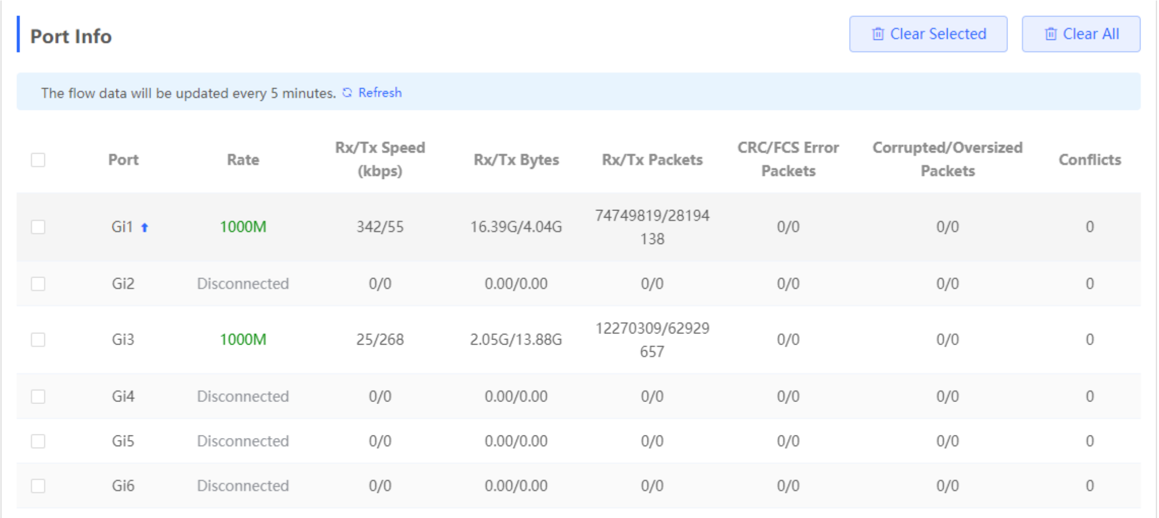
Choose **Local Device** > **Monitor** > **Port Flow**.

Display traffic statistics such as the rate of the device port, the number of sent and received packets, and the number of error packets. The rate of the port is updated every five seconds. Other traffic statistics are updated every five minutes.

Select a port and click **Clear Selected**, or click **Clear All** to clear statistics such as current port traffic and start statistics collection again.

Note

Aggregate ports can be configured. Traffic of an aggregate port is the sum of traffic of all member ports.



Port Info

The flow data will be updated every 5 minutes. Refresh

□	Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
□	Gi1 ↑	1000M	342/55	16.39G/4.04G	74749819/28194138	0/0	0/0	0
□	Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi3	1000M	25/268	2.05G/13.88G	12270309/62929657	0/0	0/0	0
□	Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

11.3 MAC Address Management

11.3.1 Overview

A MAC address table records mappings of MAC addresses and interfaces to virtual local area networks (VLANs).

A device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC Address in the packet, the device forwards the packet through the interface corresponding to the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all interfaces other than the receiving interface in broadcast mode.

MAC address entries are classified into the following types:

- Static MAC address entries: Manually configured by the user. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries does not age.
- Dynamic MAC address entries: Automatically generated by devices. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries ages.
- Filtering MAC address entries: Manually configured by the user. Packets whose source or destination MAC address matches the one in such an entry are discarded. This type of entries does not age.

Note

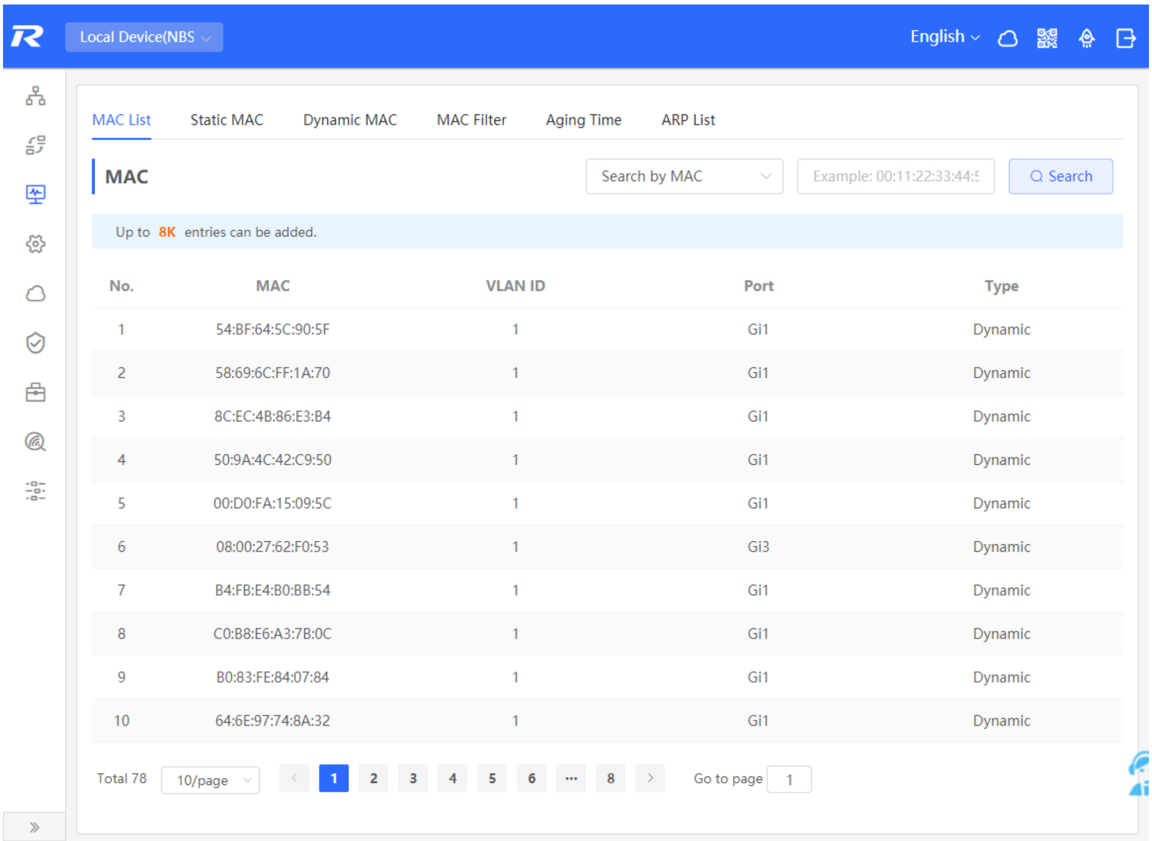
This section describes the management of static, dynamic, and filtering MAC address entries, without involving multicast MAC address entries.

11.3.2 Displaying the MAC Address Table

Choose **Local Device** > **Monitor** > **Clients** > **MAC List**.

Displays the MAC address information of the device, including the static MAC address manually set by the user, the filtering MAC address, and the dynamic MAC address automatically learned by the device.

Querying MAC address entries: Support querying MAC address entries based on MAC address, VLAN ID or port. Select the search type, enter the search string, and click **Search**. MAC entries that meet the search criteria are displayed in the list. Support fuzzy search.



MAC

Up to 8K entries can be added.

No.	MAC	VLAN ID	Port	Type
1	54:BF:64:5C:90:5F	1	Gi1	Dynamic
2	58:69:6C:FF:1A:70	1	Gi1	Dynamic
3	8C:EC:4B:86:E3:B4	1	Gi1	Dynamic
4	50:9A:4C:42:C9:50	1	Gi1	Dynamic
5	00:D0:FA:15:09:5C	1	Gi1	Dynamic
6	08:00:27:62:F0:53	1	Gi3	Dynamic
7	B4:FB:E4:B0:BB:54	1	Gi1	Dynamic
8	C0:B8:E6:A3:7B:0C	1	Gi1	Dynamic
9	B0:83:FE:84:07:84	1	Gi1	Dynamic
10	64:6E:97:74:8A:32	1	Gi1	Dynamic

Total 78 10/page 1 2 3 4 5 6 ··· 8 Go to page 1

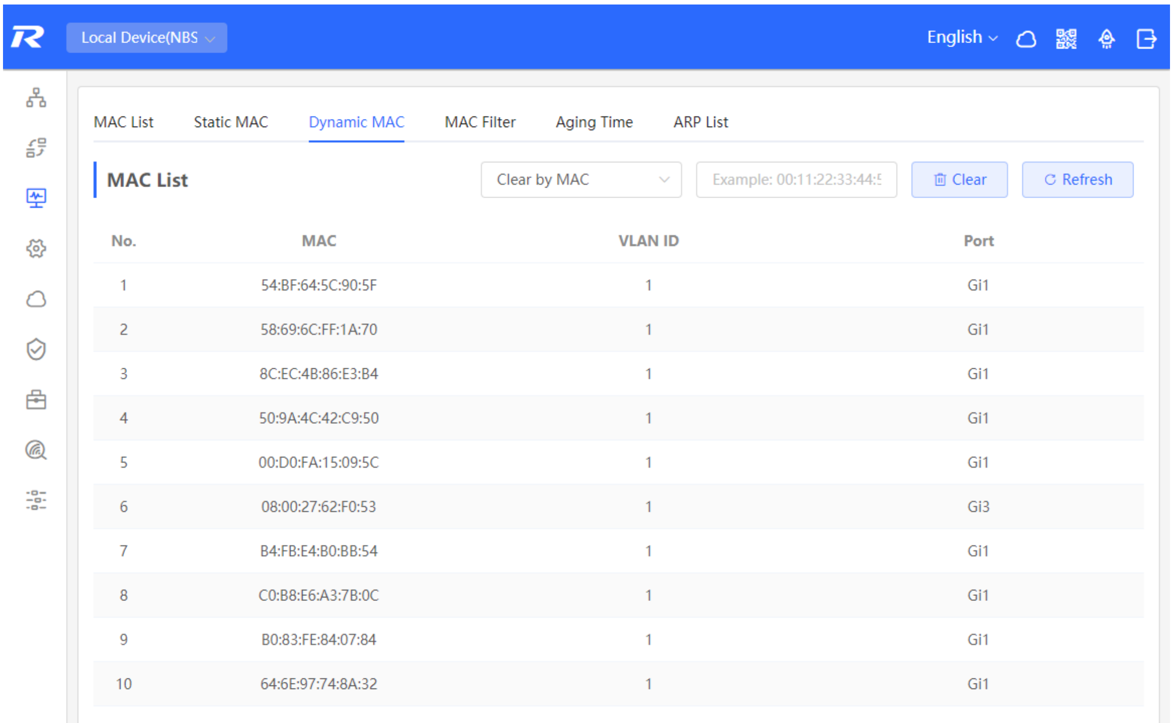
Note

The MAC address entry capacity depends on the product. For example, the MAC address entry capacity of the device shown in the figure above is 32K.

11.3.3 Displaying Dynamic MAC Address

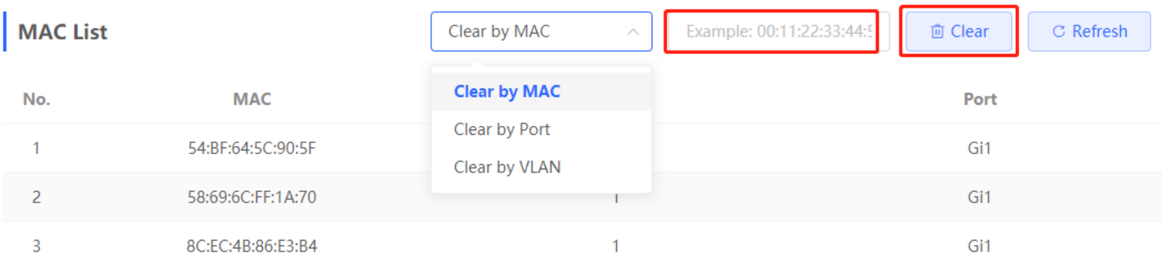
Choose **Local Device** > **Monitor** > **Clients** > **Dynamic MAC**.

After receiving the packet, the device will automatically generate dynamic MAC address entries based on the source MAC address of the packet. The current page displays the dynamic MAC address entries learned by the device. Click **Refresh** to obtain the latest dynamic MAC address entries.



No.	MAC	VLAN ID	Port
1	54:BF:64:5C:90:5F	1	Gi1
2	58:69:6C:FF:1A:70	1	Gi1
3	8C:EC:4B:86:E3:B4	1	Gi1
4	50:9A:4C:42:C9:50	1	Gi1
5	00:D0:FA:15:09:5C	1	Gi1
6	08:00:27:62:F0:53	1	Gi3
7	B4:FB:E4:B0:BB:54	1	Gi1
8	C0:B8:E6:A3:7B:0C	1	Gi1
9	B0:83:FE:84:07:84	1	Gi1
10	64:6E:97:74:8A:32	1	Gi1

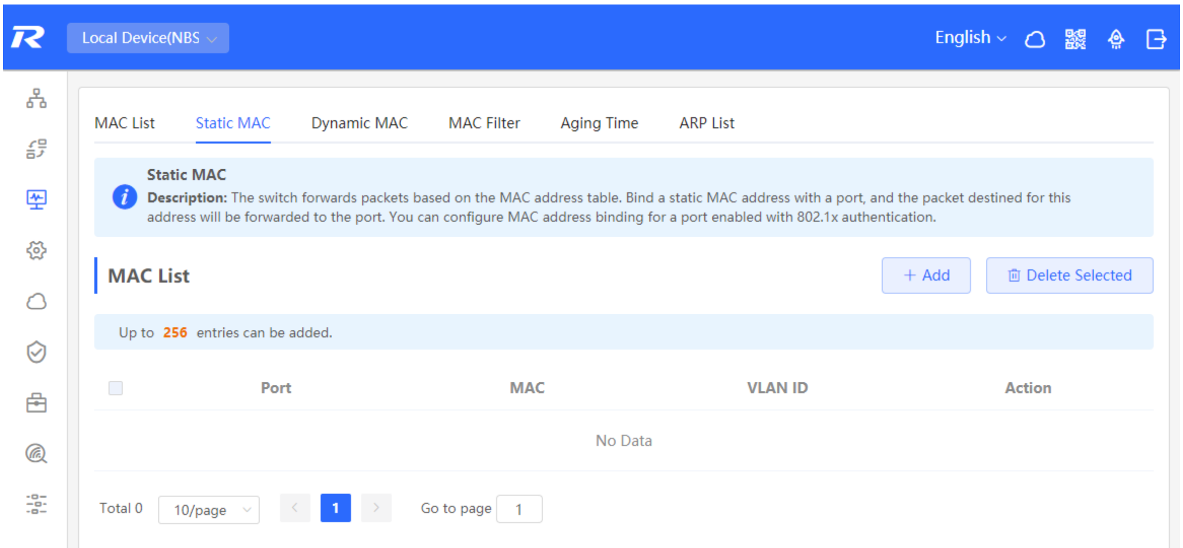
Delete dynamic MAC address: Select the clear type (by MAC address, by VLAN, or by port), enter a string for matching the dynamic MAC address entry, and click **Clear**. The device will clear MAC address entries that meet the conditions.



No.	MAC		Port
1	54:BF:64:5C:90:5F		Gi1
2	58:69:6C:FF:1A:70	1	Gi1
3	8C:EC:4B:86:E3:B4	1	Gi1

11.3.4 Configuring Static MAC Binding

The switch forwards data based on the MAC address table. You can set a static MAC address entry to manually bind the MAC address of a downlink network device with the port of the device. After a static address entry is configured, when the device receives a packet destined to this address from the VLAN, it will forward the packet to the specified port. For example, when 802.1x authentication is enabled on the port, you can configure static MAC address binding to implement authentication exemption.



Static MAC

Description: The switch forwards packets based on the MAC address table. Bind a static MAC address with a port, and the packet destined for this address will be forwarded to the port. You can configure MAC address binding for a port enabled with 802.1x authentication.

MAC List

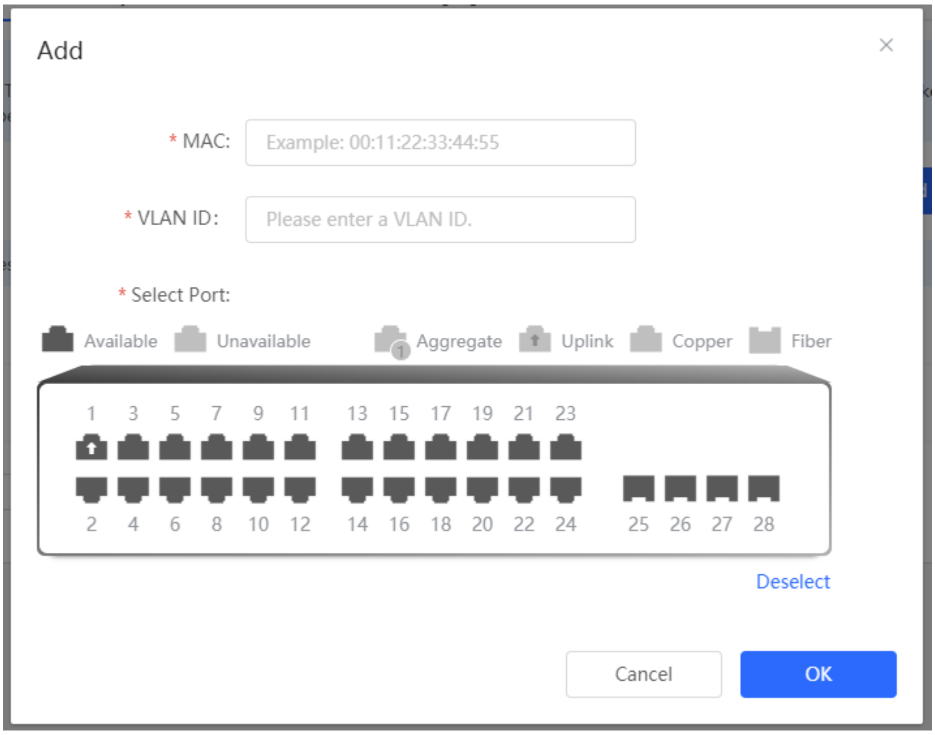
Up to 256 entries can be added.

□	Port	MAC	VLAN ID	Action
		No Data		

1. Adding Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients** > **Static MAC**.

Click **Add**, enter the MAC address and VLAN VLAN ID, select the port for packet forwarding, and click **OK**. After the addition is successful, the MAC address table will update the entry data.


Add

* MAC: Example: 00:11:22:33:44:55

* VLAN ID: Please enter a VLAN ID.

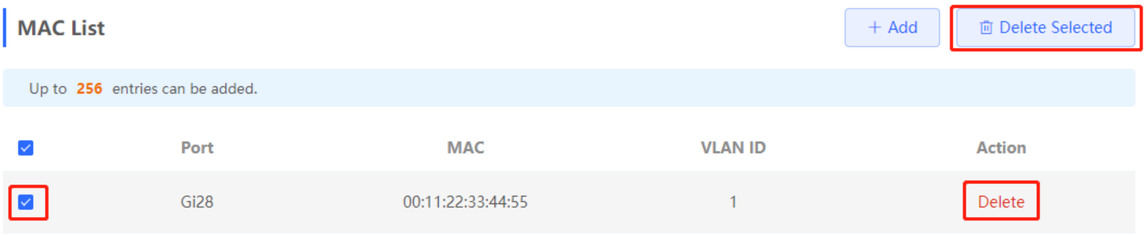
* Select Port:

2. Deleting Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients** > **Static MAC**.

Batch delete: In **MAC List**, select the MAC address entries to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.

Delete an entry: In **MAC List**, find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**.

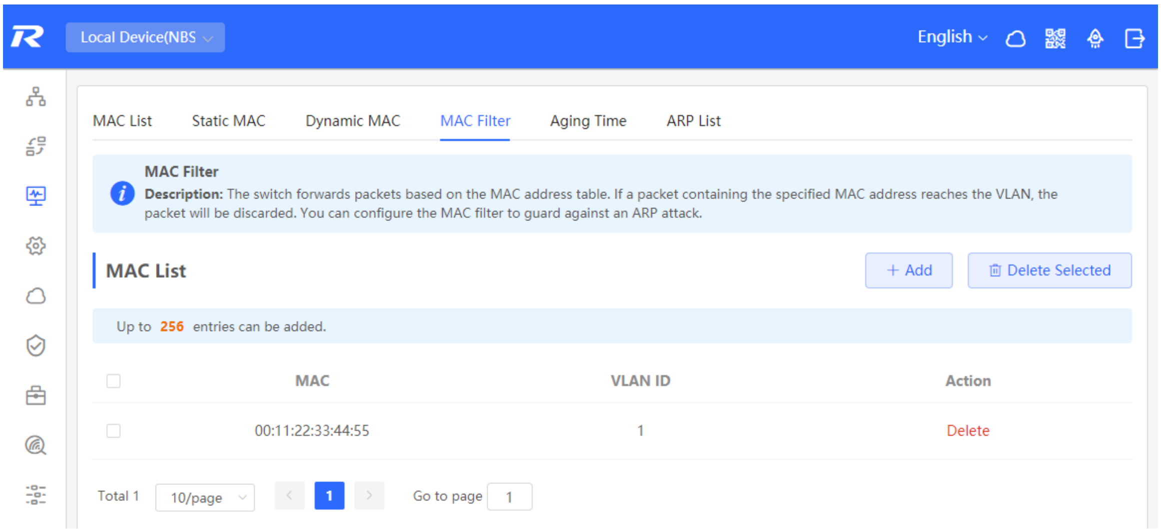


Up to 256 entries can be added.

☑	Port	MAC	VLAN ID	Action
☑	Gi28	00:11:22:33:44:55	1	Delete

11.3.5 Configuring MAC Address Filtering

To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly discarded. For example, if a user initiates ARP attacks, the MAC address of the user can be configured as a to-be-filtered address to prevent attacks.



MAC Filter

Description: The switch forwards packets based on the MAC address table. If a packet containing the specified MAC address reaches the VLAN, the packet will be discarded. You can configure the MAC filter to guard against an ARP attack.

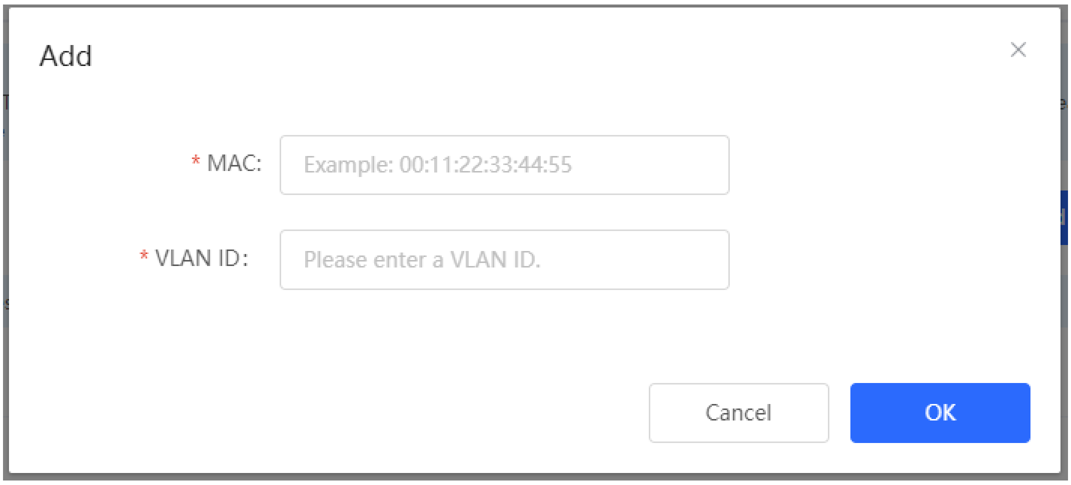
Up to 256 entries can be added.

□	MAC	VLAN ID	Action
□	00:11:22:33:44:55	1	Delete

1. Adding Filtering MAC Address

Choose **Local Device** > **Monitor** > **Clients** > **MAC Filter**.

Click **Add**. In the dialog box that appears, enter the MAC addresses and VLAN ID, and then click **OK**.



* MAC: Example: 00:11:22:33:44:55

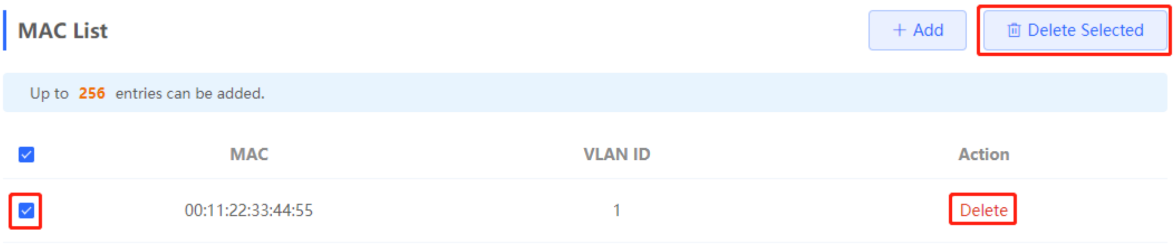
* VLAN ID: Please enter a VLAN ID.

2. MAC Filter

Choose **Local Device** > **Monitor** > **Clients** > **MAC Filter**.

Batch delete: In **MAC List**, select the MAC address entries to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.

Delete an entry: In **MAC List**, find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**.



Up to 256 entries can be added.

☑	MAC	VLAN ID	Action
☑	00:11:22:33:44:55	1	Delete

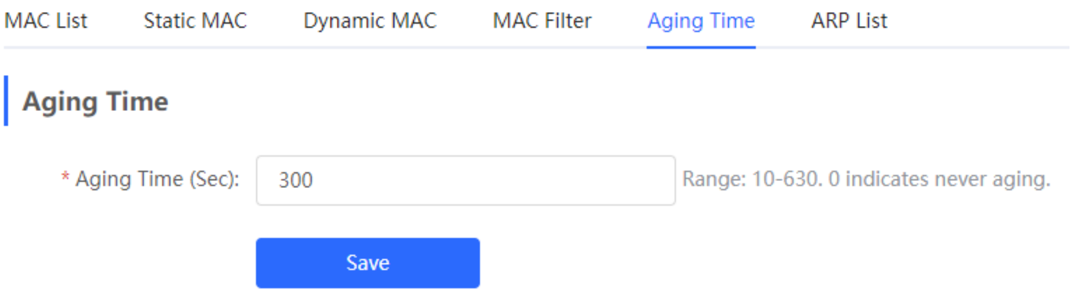
11.3.6 Configuring MAC Address Aging Time

Set the aging time of dynamic MAC address entries learned by the device. Static MAC address entries and filtering MAC address entries do not age.

The device deletes useless dynamic MAC address entries based on the aging time to save entry resources on the device. An overly long aging time may lead to untimely deletion of useless entries, whereas an overly short aging time may lead to deletion of some valid entries and repeated learning of MAC addresses by the device, which increases the packet broadcast frequency. Therefore, you are advised to configure a proper aging time of dynamic MAC address entries as required to save device resources without affecting network stability.

Choose **Local Device** > **Monitor** > **Clients** > **Aging Time**.

Enter valid aging time and click **Save**. The value range of the aging time is from 10 to 630, in seconds. The value 0 specifies no aging.



* Aging Time (Sec): 300 Range: 10-630. 0 indicates never aging.

11.4 Displaying ARP Information

Choose **Local Device** > **Monitor** > **Clients** > **ARP List**.

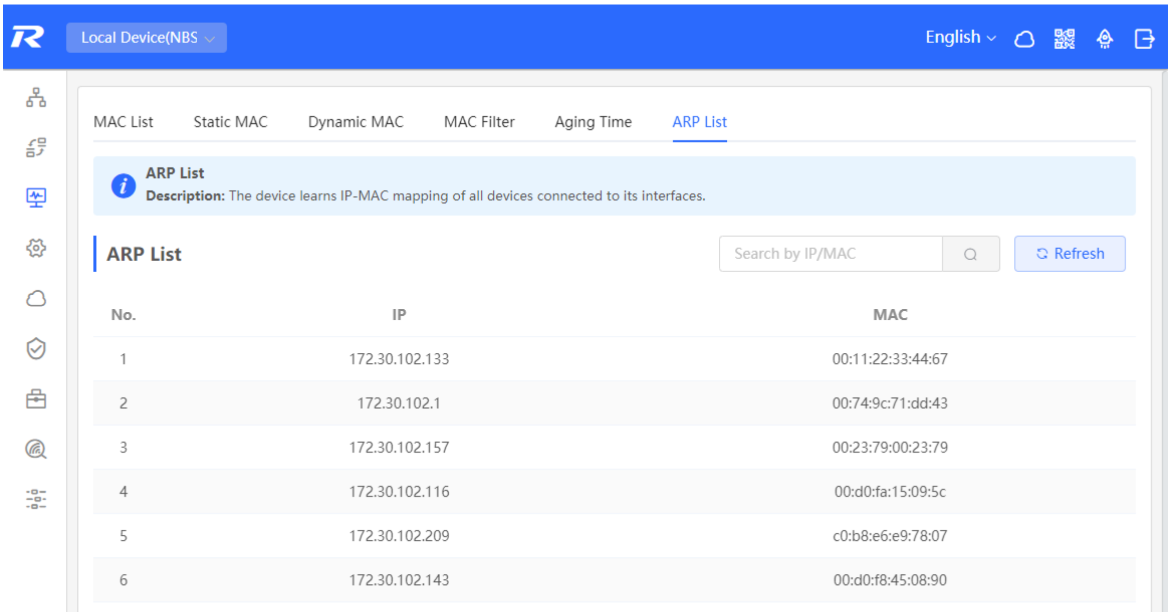
When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then send data frames to the physical network. The process of obtaining MAC addresses based on IP addresses is called address resolution.

The Address Resolution Protocol (ARP) is used to resolve IP addresses into MAC addresses. ARP can obtain the MAC Address associated with an IP address. ARP stores the mappings between IP addresses and MAC addresses in the ARP cache of the device.

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. The **ARP List** page displays ARP entries learned by the device. The ARP list allows you search for specified ARP entries by IP or MAC address. Click **Refresh** to obtain the latest ARP entries.

Note

For more ARP entry function introduction, see 14.4 .



ARP List
Description: The device learns IP-MAC mapping of all devices connected to its interfaces.

ARP List

No.	IP	MAC
1	172.30.102.133	00:11:22:33:44:67
2	172.30.102.1	00:74:9c:71:dd:43
3	172.30.102.157	00:23:79:00:23:79
4	172.30.102.116	00:d0:fa:15:09:5c
5	172.30.102.209	c0:b8:e6:e9:78:07
6	172.30.102.143	00:d0:f8:45:08:90

11.5 VLAN

11.5.1 VLAN Overview

A virtual local area network (VLAN) is a logical network created on a physical network. A VLAN has the same properties as a normal physical network except that it is not limited by its physical location. Each VLAN has an independent broadcast domain. Different VLANs are L2-isolated. L2 unicast, broadcast, and multicast frames are forwarded and spread within one VLAN and will not be transmitted to other VLANs.

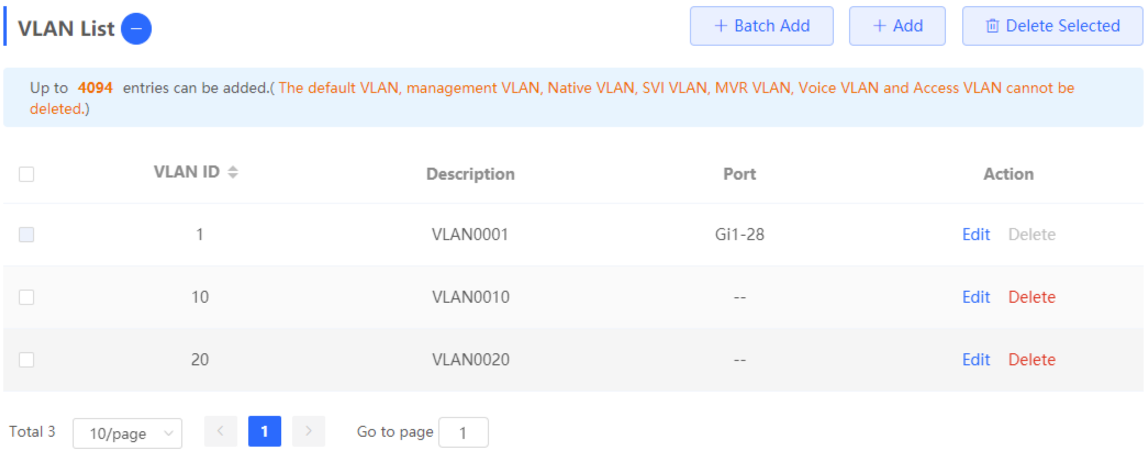
When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs. VLANs can make L3 communication with each other through L3 devices or L3 interfaces.

VLAN division includes two functions: creating VLANs and setting port VLANs.

11.5.2 Creating a VLAN

Choose **Local Device** > **VLAN** > **VLAN List**.

The VLAN list contains all the existing VLAN information. You can modify or delete the existing VLAN, or create a new VLAN.

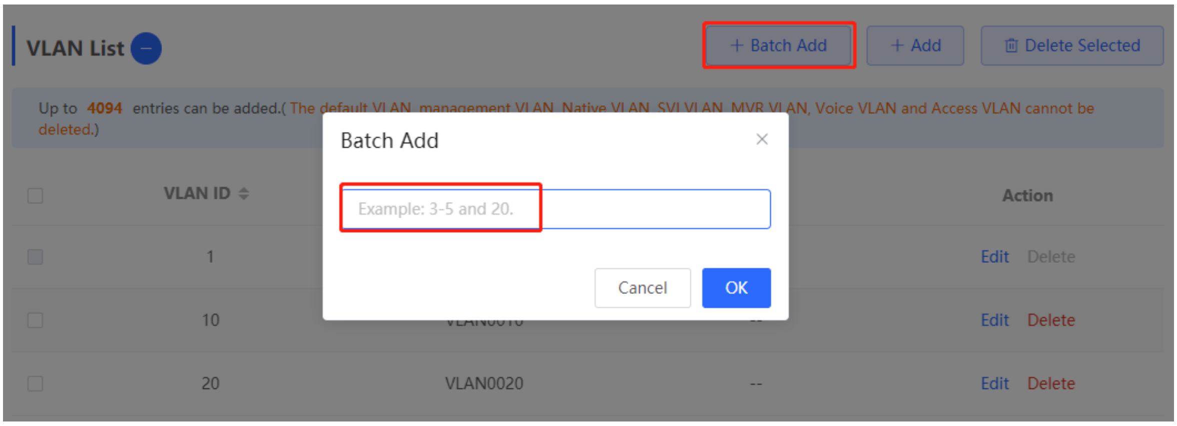


Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

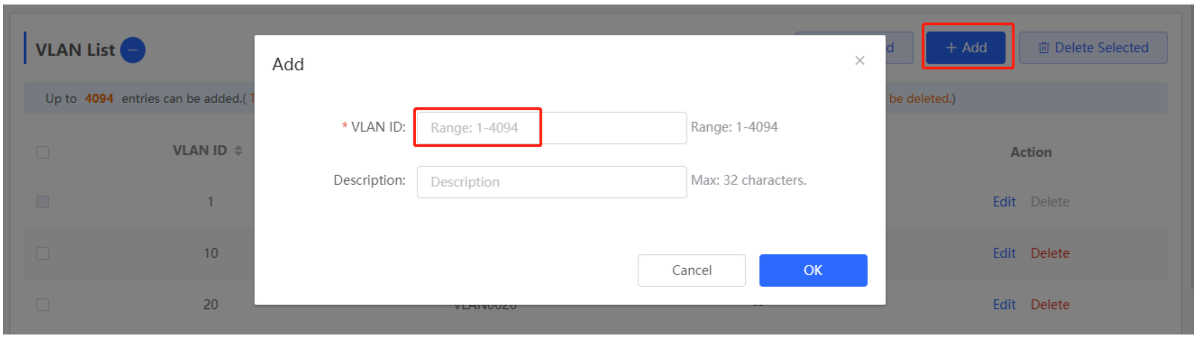
□	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi1-28	Edit Delete
□	10	VLAN0010	--	Edit Delete
□	20	VLAN0020	--	Edit Delete

1. Adding a VLAN

Create multiple VLANs: Click **Batch Add**. In the displayed dialog box, enter VLAN ID range (separate multiple VLAN ID ranges with commas (,)), and click **OK**. The VLANs added will be displayed in **VLAN List**.



Create a VLAN: Click **Add**. Enter the VLAN ID and description for the VLAN, and click **OK**. The VLAN added will be displayed in **VLAN List**.



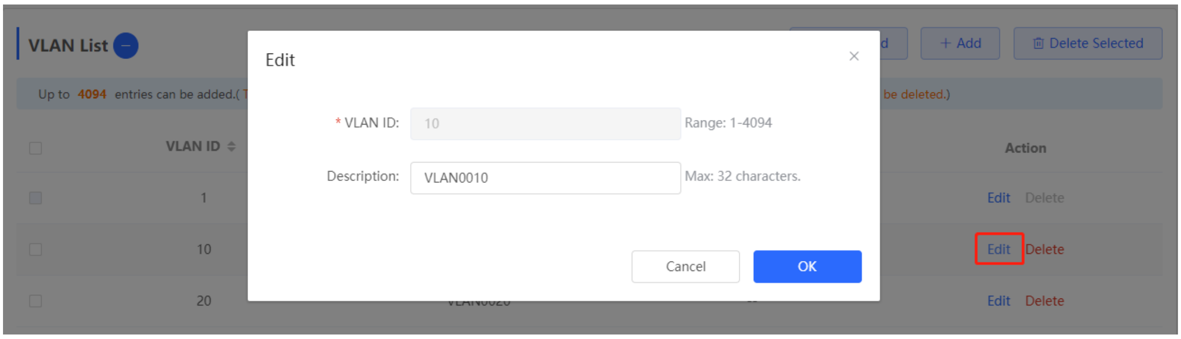
Note

- The range of a VLAN ID is from 1 to 4094.
- You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).
- If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.

- If the device supports L3 functions, VLANs, routed ports, and L3 aggregate ports (L3APs) share limited hardware resources. If resources are insufficient, a message indicating resource insufficiency for VLAN will be displayed.

2. VLAN Description Modifying

In **VLAN List**, Click **Edit** in the last **Action** column to modify the description information of the specified VLAN.



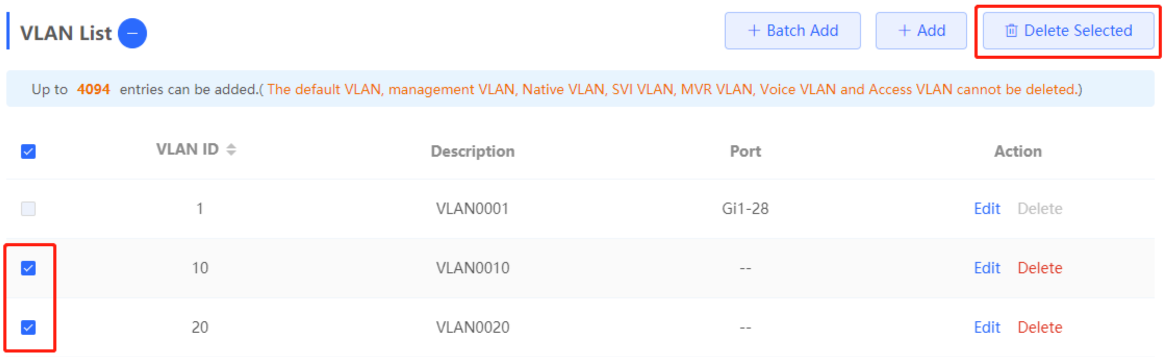
Edit

* VLAN ID: 10 Range: 1-4094

Description: VLAN0010 Max: 32 characters.

3. Deleting a VLAN

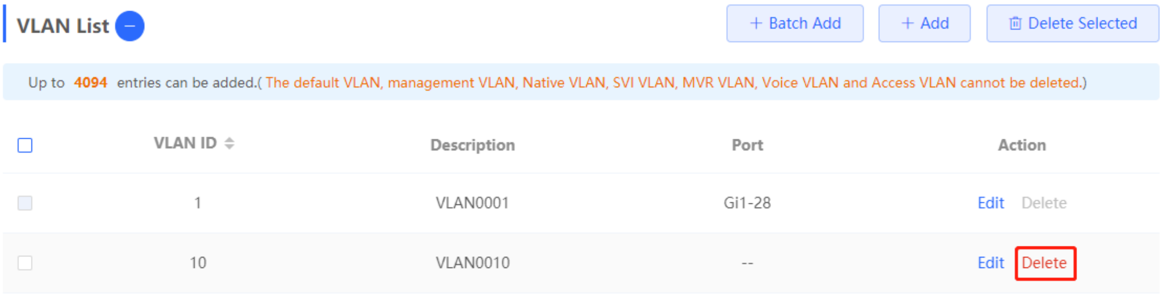
Batch delete VLANs: In **VLAN List**, select the VLAN entries to be deleted and click **Delete Selected** to delete VLANs in a batch.



Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

☑	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi1-28	Edit Delete
☑	10	VLAN0010	--	Edit Delete
☑	20	VLAN0020	--	Edit Delete

Delete a VLAN: In **VLAN List**, click **Delete** in the last **Action** column to delete the specified **VLAN**.



Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

□	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi1-28	Edit Delete
□	10	VLAN0010	--	Edit Delete

Note

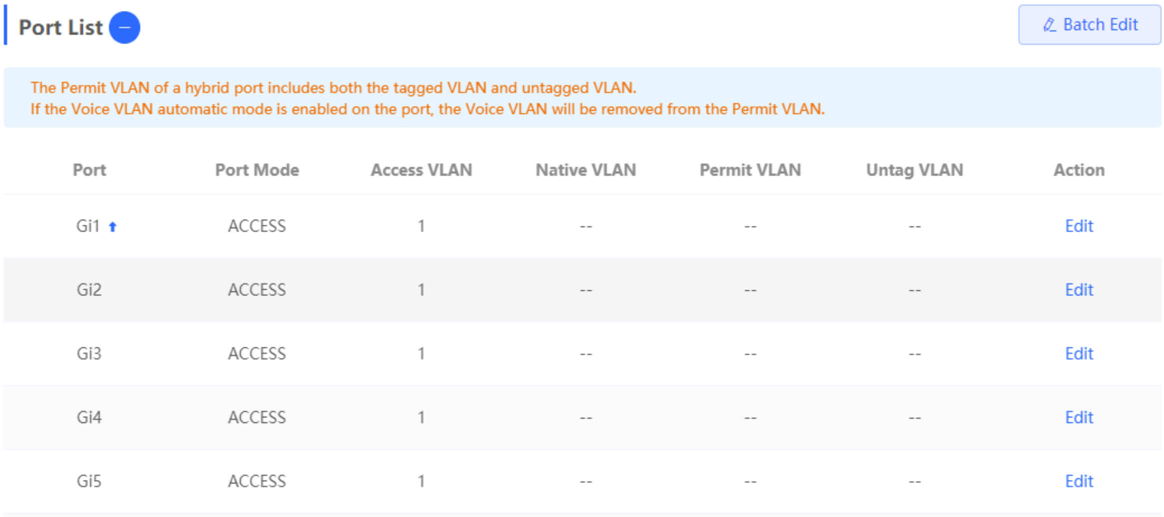
The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. For these VLANs, the **Delete** button is unavailable in gray.

11.5.3 Configuring Port VLAN

1. Overview

Choose **Local Device** > **VLAN** > **Port List**.

Port List displays the VLAN division of the current port. Create VLANs in **VLAN List** page (see 3.5.2Creating a VLAN) and then configure the port based on the VLANs.



The Permit VLAN of a hybrid port includes both the tagged VLAN and untagged VLAN.
If the Voice VLAN automatic mode is enabled on the port, the Voice VLAN will be removed from the Permit VLAN.

Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Untag VLAN	Action
Gi1	ACCESS	1	--	--	--	Edit
Gi2	ACCESS	1	--	--	--	Edit
Gi3	ACCESS	1	--	--	--	Edit
Gi4	ACCESS	1	--	--	--	Edit
Gi5	ACCESS	1	--	--	--	Edit

You can configure the port mode and VLAN members for a port to determine VLANs that are allowed to pass through the port and whether packets to be forwarded by the port carry the tag field.

Table 11-1 Port Modes Description

Port mode	Function
Access port	One access port can belong to only one VLAN and allow only frames from this VLAN to pass through. This VLAN is called an access VLAN. Access VLAN has attributes of both Native VLAN and Permitted VLAN The frames sent from the Access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the Access VLAN and adds the access VLAN ID to the frame.
Trunk port	One trunk port supports one native VLAN and several allowed VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while allowed VLAN frames forwarded by the trunk port carry tags. A trunk port belongs to all VLANs of the device by default, and can forward frames of all VLANs. You can set the allowed VLAN range to limit VLAN frames that can be forwarded. Note that the trunk ports on both ends of the link must be configured with the same Native VLAN.
Hybrid port	A hybrid port supports one native VLAN and several allowed VLANs. The allowed VLANs are divided into Tag VLAN and Untag VLAN. The frames forwarded by the hybrid port from a Tag VLAN carry tags, and the frames forwarded by the hybrid port from an Untag VLAN do not carry tags. The frames forwarded by the hybrid port from Native VLAN must not carry tags,

Port mode	Function
	therefore Native VLAN can only belong to Untag VLAN List.

Note

Whether the hybrid mode function is supported depends on the product version.

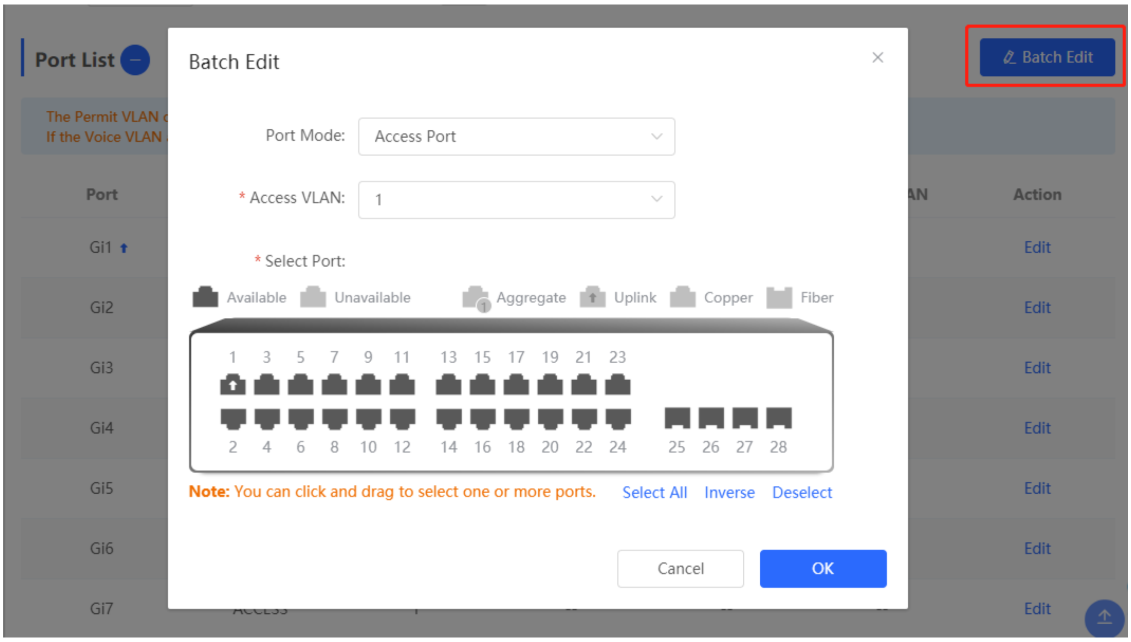
2. Procedure

Choose **Local Device** > **VLAN** > **Port List**.

Configure port VLANs in a batch: Click **Batch Edit**, select the port to be configured on the port panel, and select the port mode. If the port mode is Access port, you need to select Access VLAN; if the port mode is Trunk port, you need to select Native VLAN and enter the allowed VLAN ID range; if the port mode is Hybrid port, you need to select Native VLAN and enter the allowed VLAN range and Untag VLAN range. Click **OK** to complete the batch configuration.

Note

In Hybrid mode, the allowed VLANs include Tag VLAN and Untag VLAN, and the Untag VLAN range must include Native VLAN.



Batch Edit

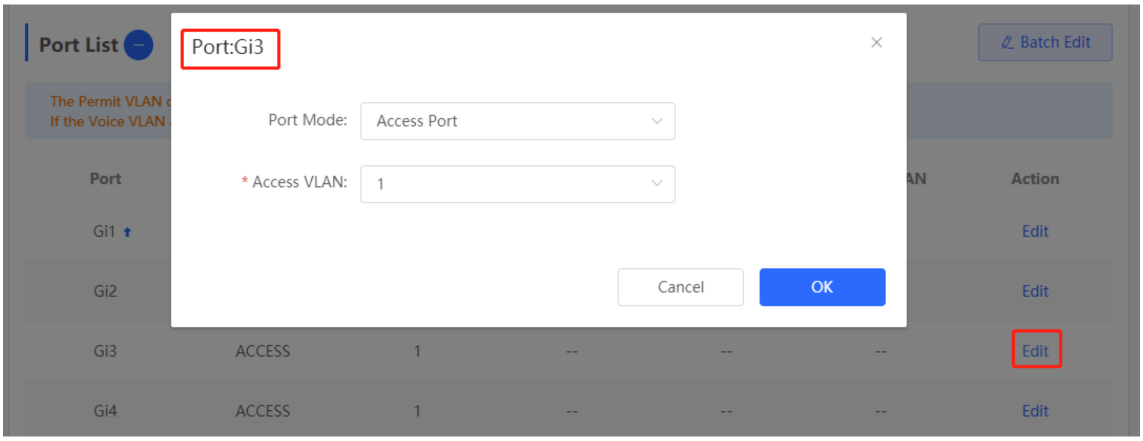
Port Mode: Access Port

* Access VLAN: 1

* Select Port:

Note: You can click and drag to select one or more ports.

Configure one port: In **Port List**, click **Edit** in the last **Action** column of a specified port, configure the port mode and corresponding VLAN, and click **OK**.



Port:Gi3

Port Mode: Access Port

* Access VLAN: 1

Cancel OK

Note

- VLAN ID range is from 1 to 4094, among which VLAN 1 is the default VLAN that cannot be deleted.
- When hardware resources are insufficient, the system displays a VLAN creation failure message.
- Improper configuration of VLANs on a port (especially uplink port) may cause the failure to log in to the Eweb management system. Therefore, exercise caution when configuring VLANs.

11.5.4 Batch Switch Configuration

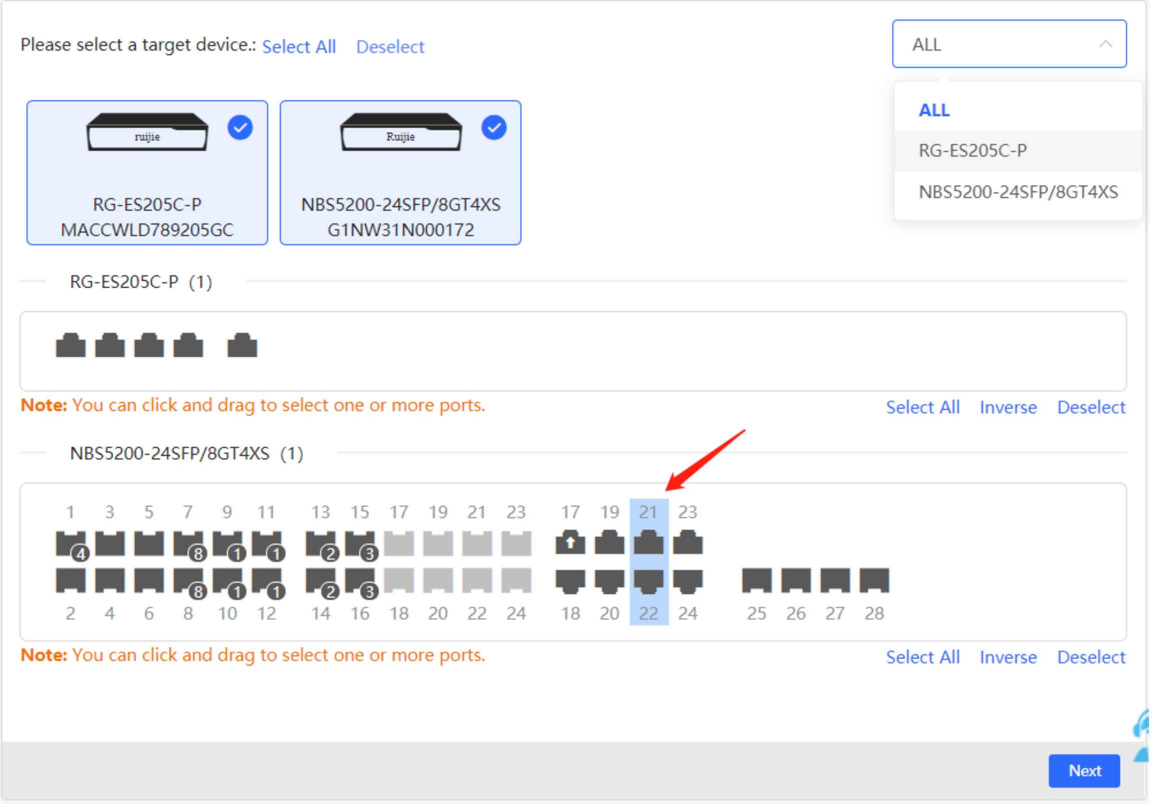
1. Overview

You can batch create VLANs, configure port attributes, and divide port VLANs for switches in the network.

2. Procedure

Choose **Network** > **Batch Config**.

(1) The page displays all switches in the current network. Select the switches to configure, and then select the desired ports in the device port view that appears below. If there are a large number of devices in the current network, select a product model from the drop-down list box to filter the devices. After the desired devices and ports are selected, click **Next**.



Please select a target device.: Select All Deselect

ALL

ALL
RG-ES205C-P
NBS5200-24SFP/8GT4XS

RG-ES205C-P
MACCWLD789205GC

NBS5200-24SFP/8GT4XS
G1NW31N000172

RG-ES205C-P (1)

Note: You can click and drag to select one or more ports.

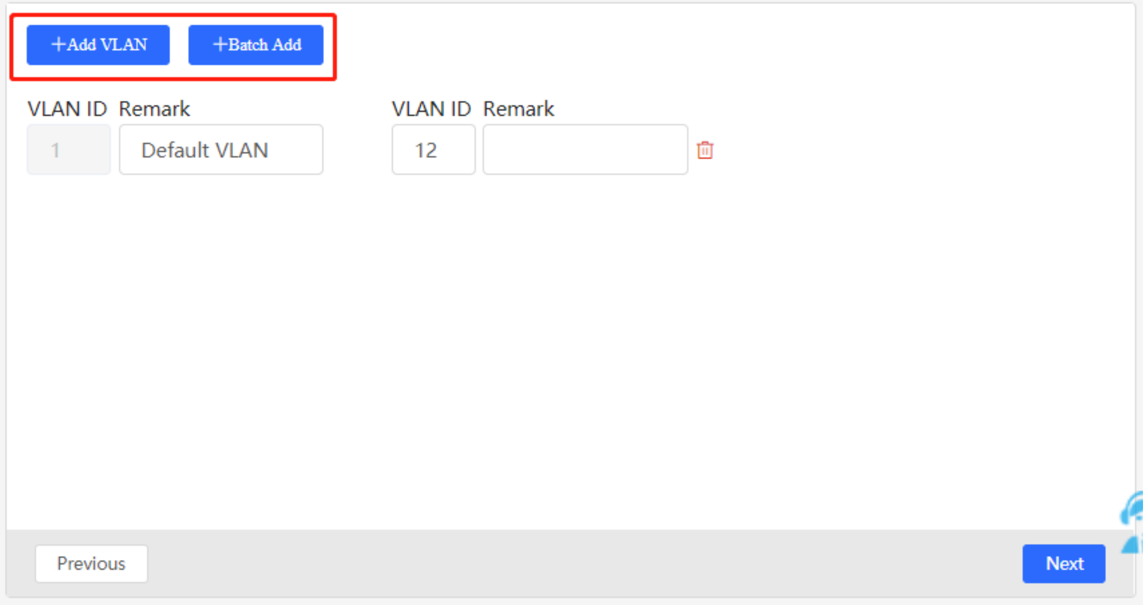
Select All Inverse Deselect

NBS5200-24SFP/8GT4XS (1)

Note: You can click and drag to select one or more ports.

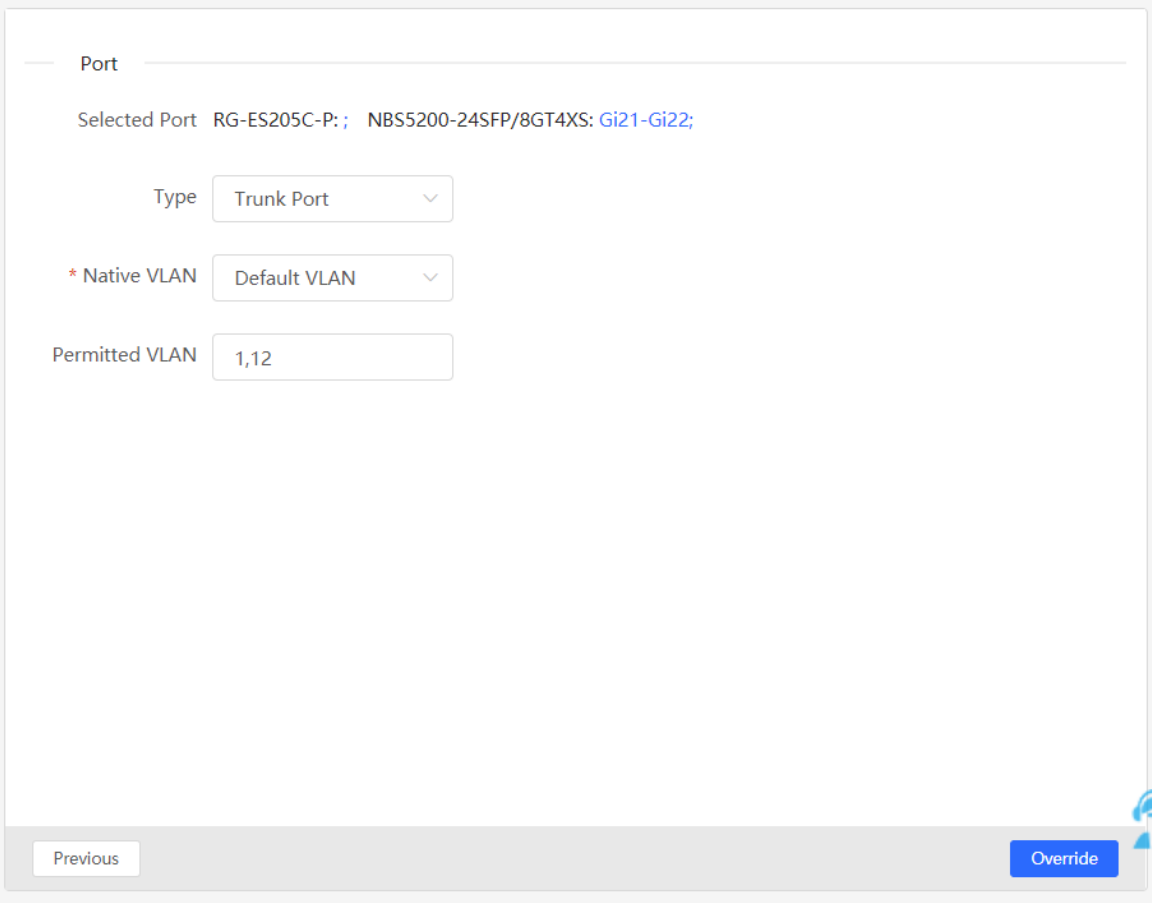
Select All Inverse Deselect

(2) Click **Add VLAN** to create a VLAN for the selected devices in a batch. If you want to create multiple VLANs, click **Batch Add** and enter the VLAN ID range, such as 3-5,100. After setting the VLANs, click **Next**.



VLAN ID	Remark	VLAN ID	Remark
1	Default VLAN	12	

(3) Configure port attributes for the ports selected in Step 1 in a batch. Select a port type. If you set **Type** to **Access Port**, you need to configure **VLAN ID**. If you set **Type** to **Trunk Port**, you need to configure **Native VLAN** and **Permitted VLAN**. After setting the port attributes, click **Override** to deliver the batch configurations to the target devices.



Port

Selected Port RG-ES205C-P: ; NBS5200-24SFP/8GT4XS: Gi21-Gi22;

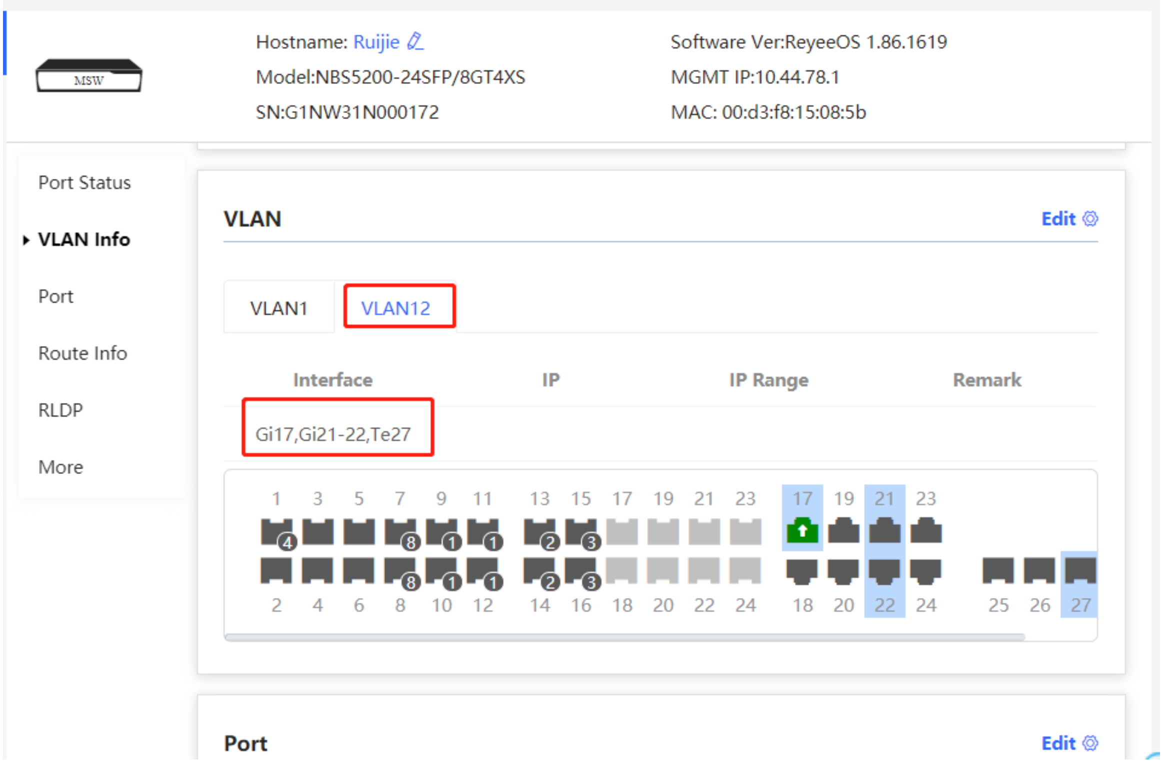
Type: Trunk Port

* Native VLAN: Default VLAN

Permitted VLAN: 1,12

11.5.5 Verifying Configuration

View the VLAN and port information of switches to check whether the batch configurations are successfully delivered.



Hostname: Ruijie

Model:NBS5200-24SFP/8GT4XS

SN:G1NW31N000172

Software Ver:ReyeeOS 1.86.1619

MGMT IP:10.44.78.1

MAC: 00:d3:f8:15:08:5b

Interface	IP	IP Range	Remark
Gi17,Gi21-22,Te27			

12 NBS Series Port Management

12.1 Overview

Ports are important components for data exchange on network devices. The port management module allows you to configure basic settings for ports, and configure port aggregation, switched port analyzer (SPAN), port rate limiting, management IP address, etc.

Table 4-1 Description of Port Type

Port Type	Note	Remarks
Switch Port	A switch port consists of a single physical port on the device and provides only the L2 switching function. Switch ports are used to manage physical port and their associated L2 protocols.	Described in this section
L2 aggregate port	An Interface binds multiple physical members to form a logical link. For L2 switching, an aggregate port is like a high-bandwidth switch port. It can combine the bandwidths of multiple ports to expand link bandwidth. In addition, for frames sent through an L2 aggregate port, load balancing is performed on member ports of the L2 aggregate port. If one member link of the aggregate port fails, the L2 aggregate port automatically transfers traffic on this link to other available member links, improving connection reliability.	Described in this section
SVI Port	A switch virtual interface (SVI) serves as the management interface of the device, through which the device can be managed. You can also create an SVI as a gateway interface, which is equivalent to the virtual interface of corresponding VLAN and can be used for inter-VLAN routing on L3 devices.	For related configuration, see 6.1
Routed Port	On L3 devices, you can configure a single physical port as a routed port and use it as the gateway interface of L3 switching. Route interfaces do not have L2 switching functions and have no corresponding relationship with VLANs, but only serve as access interfaces.	For related configuration, see 6.1

Port Type	Note	Remarks
L3 Aggregate Port	An L3 aggregate port is a logical aggregate port group composed of multiple physical member ports, just like an L2 aggregate port. The ports to be aggregated must be L3 ports of the same type. An aggregate port serves as the gateway interface of L3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections. L3 aggregate ports do not support the L2 switching function.	For related configuration, see 6.1

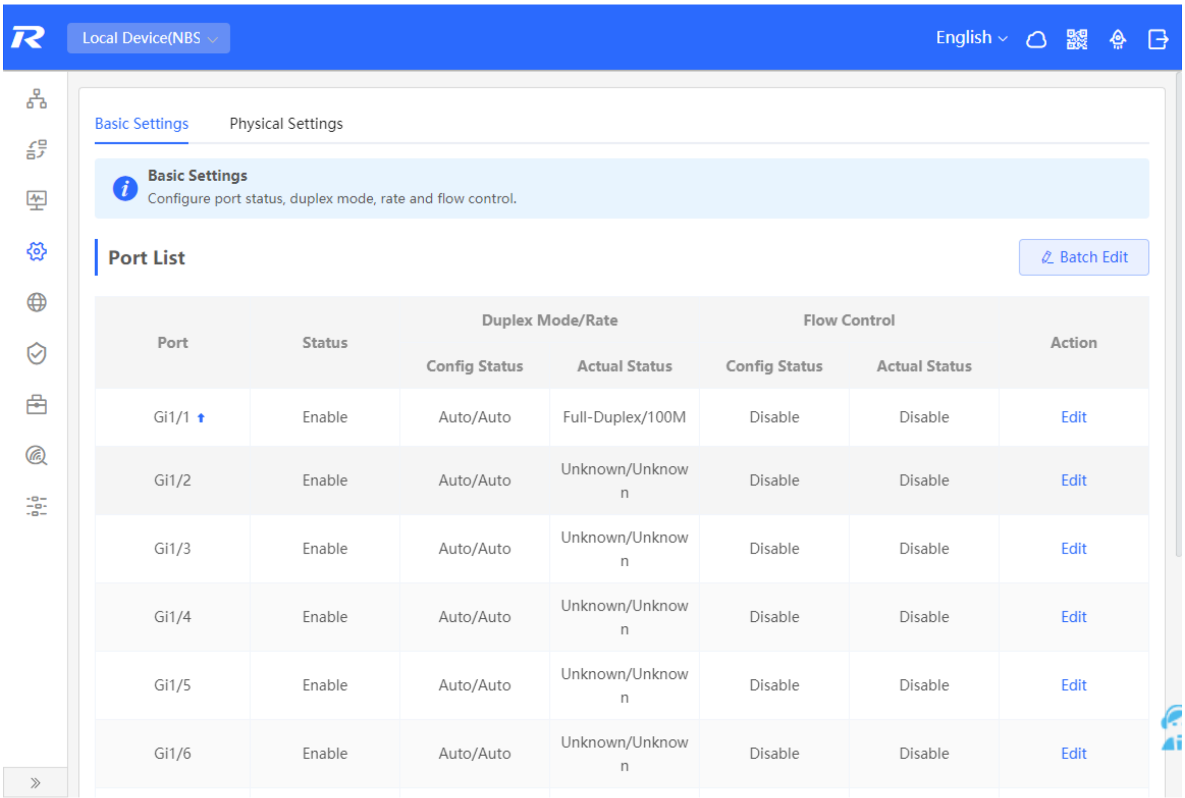
12.2 Port Configuration

Port configuration includes common attributes such as basic settings and physical settings of the port. Users can adjust the port rate, set port switch, duplex mode, flow control mode, energy efficient Ethernet switch, port media type and MTU, etc.

12.2.1 Basic Settings

Choose **Local Device** > **Ports** > **Basic Settings** > **Basic Settings**.

Support setting whether to enable the port, the speed and duplex mode of the port, and the flow control mode, and display the current actual status of each port.

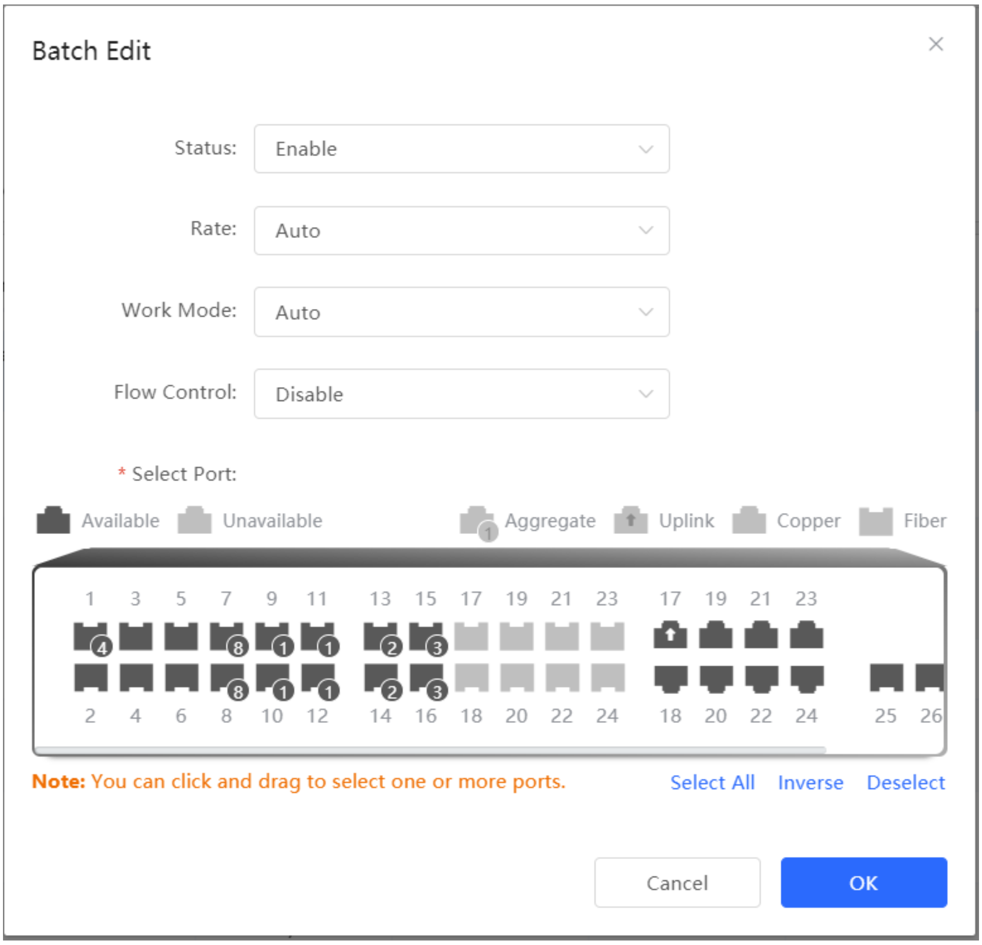


Basic Settings
Configure port status, duplex mode, rate and flow control.

Port List

Port	Status	Duplex Mode/Rate		Flow Control		Action
		Config Status	Actual Status	Config Status	Actual Status	
Gi1/1 ↑	Enable	Auto/Auto	Full-Duplex/100M	Disable	Disable	Edit
Gi1/2	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi1/3	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi1/4	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi1/5	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi1/6	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit

Batch configure: Click **Batch Edit**, select the port to be configured In the displayed dialog box, select the port switch, rate, work mode, and flow control mode, and click **OK** to deliver the configuration. In batch configuration, optional configuration items are a common collection of selected ports (that is, attributes supported the selected ports).



Batch Edit

Status: Enable

Rate: Auto

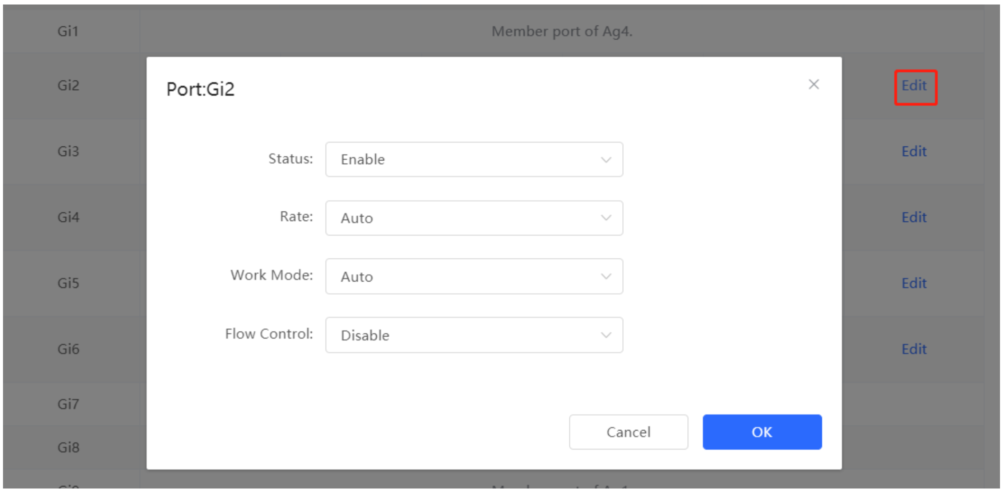
Work Mode: Auto

Flow Control: Disable

* Select Port:

Note: You can click and drag to select one or more ports.

Configure one port: In **Port List**, select a port entry and click **Edit** in the **Action** column. In the displayed dialog box, select port status, rate, work mode, and flow control mode, and click **OK**.



Gi1 Member port of Ag4.

Port:Gi2

Status: Enable

Rate: Auto

Work Mode: Auto

Flow Control: Disable

Table 4-2 Description of Basic Port Configuration Parameters

Parameter	Description	Default Value
Status	If a port is closed, no frame will be received and sent on this port, and the corresponding data processing function will be lost, but the PoE power supply function of the port will not be	Enable

Parameter	Description	Default Value
	affected.	
Rate	Set the rate at which the Ethernet physical interface works. Set to Auto means that the port rate is determined by the auto-negotiation between the local and peer devices. The negotiated rate can be any rate within the port capability.	Auto
Work Mode	Full duplex: realize that the port can receive packets while sending. Half duplex: control that the port can receive or send packets at a time. Auto: the duplex mode of the port is determined through auto negotiation between the local port and peer port	Auto
Flow Control	After flow control is enabled, the port will process the received flow control frames, and send the flow control frames when congestion occurs on the port.	Disable

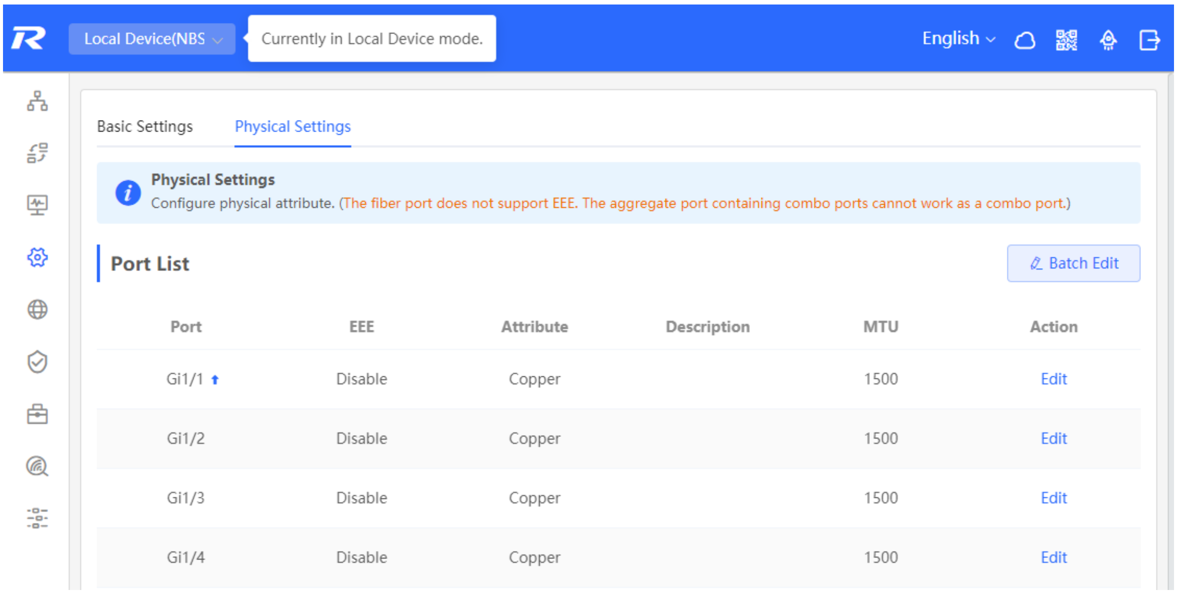
Note

The rate of a GE port can be set to 1000M, 100M, or auto. The rate of a 10G port can be set to 10G, 1000M, or auto.

12.2.2 Physical Settings

Choose **Local Device** > **Ports** > **Basic Settings** > **Physical Settings**.

Support to enable the energy-efficient Ethernet (EEE) function of the port, and set the media type and MTU of the port.



Physical Settings

Configure physical attribute. (The fiber port does not support EEE. The aggregate port containing combo ports cannot work as a combo port.)

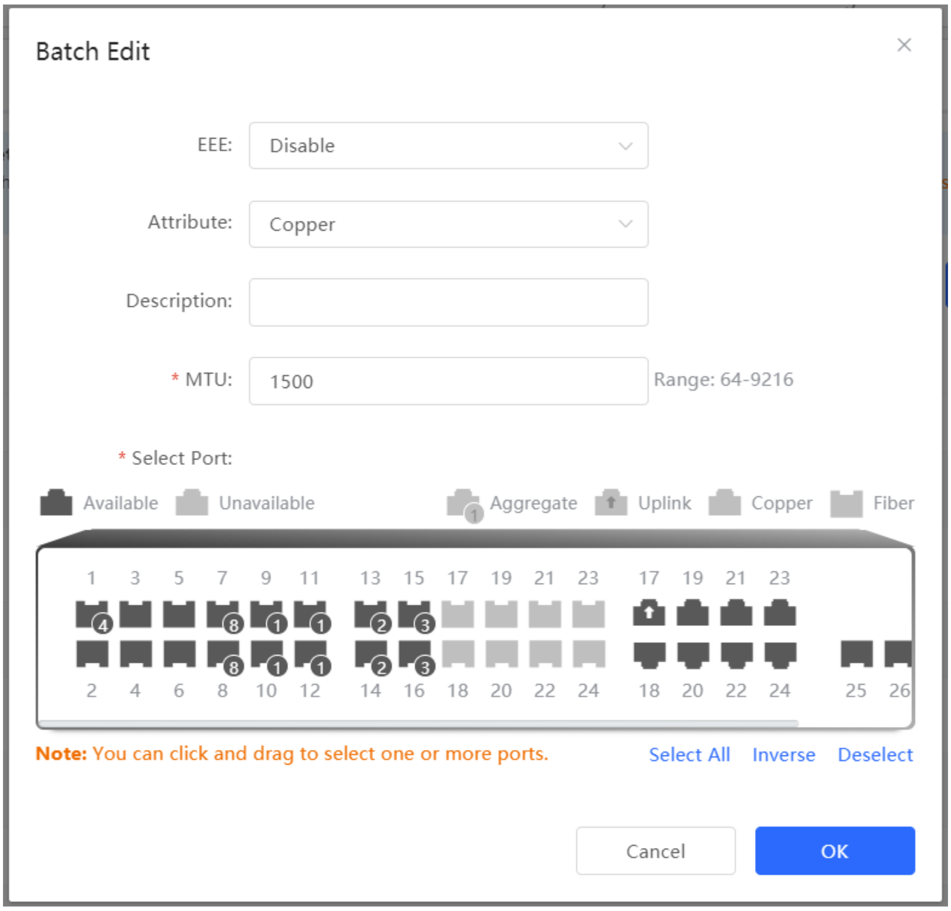
Port List

Port	EEE	Attribute	Description	MTU	Action
Gi1/1 ↑	Disable	Copper		1500	Edit
Gi1/2	Disable	Copper		1500	Edit
Gi1/3	Disable	Copper		1500	Edit
Gi1/4	Disable	Copper		1500	Edit

Batch configure: Click **Batch Edit**. In the displayed dialog box, select the port to be configured, configure the EEE switch, MTU, enter the port description, and click **OK**.

Note

Copper ports and SFP ports cannot be both configured during batch configuration.



Batch Edit

EEE: Disable

Attribute: Copper

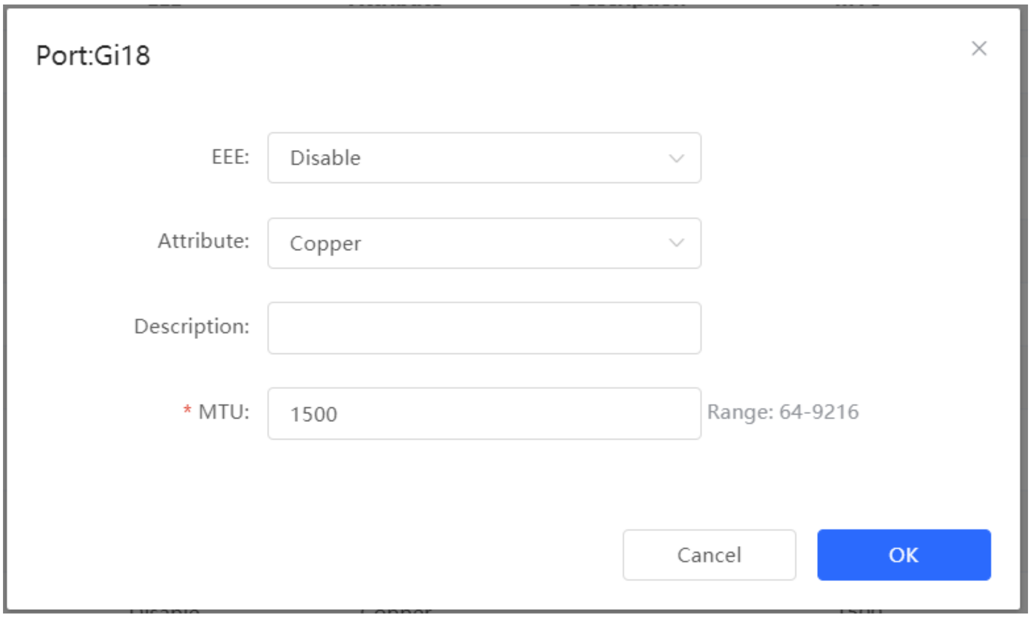
Description:

* MTU: 1500 Range: 64-9216

* Select Port:

Note: You can click and drag to select one or more ports.

Configure one port: Click **Edit** in the **Action** column of the list. In the displayed configuration box, configure the EEE switch, port mode, enter the port description, and click **OK**.



Port:Gi18

EEE: Disable

Attribute: Copper

Description:

* MTU: 1500 Range: 64-9216

Table 4-3 Description of Physical Configuration Parameters

Parameter	Description	Default Value
EEE	It is short for energy-efficient Ethernet, which is based on the standard IEEE 802.3az protocol. When enabled, EEE saves energy by making the interface enter LPI (Low Power Idle) mode when the Ethernet connection is idle. Value: Disable/Enable	Disable

Attribute	The port attribute indicates whether the port is a copper port or an SFP port.
	Coper port: copper mode (cannot be changed);
	SFP port: fiber mode (cannot be changed);
	Only combo ports support mode change.
		Depending on the port attribute

Description	You can add a description to label the functions of a port.	NA
MTU	MTU (Maximum Transmission Unit) is used to notify the peer of the acceptable maximum size of a data service unit. It indicates the size of the payload acceptable to the sender.. You can configure the MTU of a port to limit the length of a frame that can be received or forwarded through this port.	1500

Note

- Different ports support different attributes and configuration items.
- Only the SFP combo ports support port mode switching.
- SFP ports do not support enabling EEE.

12.3 Aggregate Ports

12.3.1 Aggregate Port Overview

An aggregate port (AP) is a logical link formed by binding multiple physical links. It is used to expand link bandwidth, thereby improving connection reliability.

The AP function supports load balancing and therefore, evenly distributes traffic to member links. The AP implements link backup. When a member link of an AP is disconnected, the system automatically distributes traffic of this link to other available member links. Broadcast or multicast packets received by one member link of an AP are not forwarded to other member links.

- If a single interface that connects two devices supports the maximum rate of 1000 Mbps (assume that interfaces of both devices support the rate of 1000 Mbps), when the service traffic on the link exceeds 1000 Mbps, the excess traffic will be discarded. Link aggregation can solve this problem. For example, use *n* network cables to connect the two devices and bind the interfaces together. In this way, the interfaces are logically bound to support the maximum traffic of 1000 Mbps × *n*.
- If two devices are connected through a single cable, when the link between the two interfaces is disconnected, services carried on this link are interrupted. After multiple interconnected interfaces are bound, as long as there is one link available, services carried on these interfaces will not be interrupted.

12.3.2 Overview

1. Static AP Address

In static AP mode, you can manually add a physical interface to an aggregate port. An aggregate port in static AP mode is called a static aggregate port and the member ports are called member ports of the static aggregate port. Static AP can be easily implemented. You can aggregate multiple physical links by running commands to add specified physical interfaces to an AP. Once a member interface is added to an AP, it can send and receive data and balance traffic in the AP.

2. Dynamic Aggregation

Dynamic aggregation mode is a special port aggregation function developed for the WAN port of RG-MR series gateway devices. The maximum bandwidth of the WAN port of the MR device can support 2000M, but after the intranet port is connected to the switch, a single port can only support a maximum bandwidth of 1000M. In order to prevent the downlink bandwidth from being wasted, it is necessary to find a way to increase the maximum bandwidth of the port between the MR device and the switch, and the dynamic aggregation function emerged to meet the need.

After connecting the two fixed AG (aggregation) member ports on the MR gateway device to any two ports on the switch, through packet exchange, the two ports on the switch can be automatically aggregated, thereby doubling the bandwidth. The aggregate port automatically generated in this way on the switch is called a dynamic aggregate port, and the corresponding two ports are the member ports of the aggregate port.

Note

Dynamic aggregate ports do not support manual creation and can be deleted after they are automatically generated by the device, but member ports cannot be modified.

3. Load Balancing

An AP, based on packet characteristics such as the source MAC address, destination MAC address, source IP address, destination IP address, L4 source port ID, and L4 destination port ID of packets received by an inbound interface, differentiates packet flows according to one or several combined algorithms. It sends the same packet flow through the same member link, and evenly distributes different packet flows among member links. For example, in load balancing mode based on source MAC addresses, packets are distributed to different member links of an AP based on their source MAC addresses. Packets with different source MAC addresses are distributed to different member links; packets with a same source MAC address are forwarded along a same member link.

Currently, the AP supports the traffic balancing modes based on the following:

- 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
- Source port
- L4 source port or L4 destination port
- L4 source port + L4 destination port

12.3.3 Aggregate Port Configuration

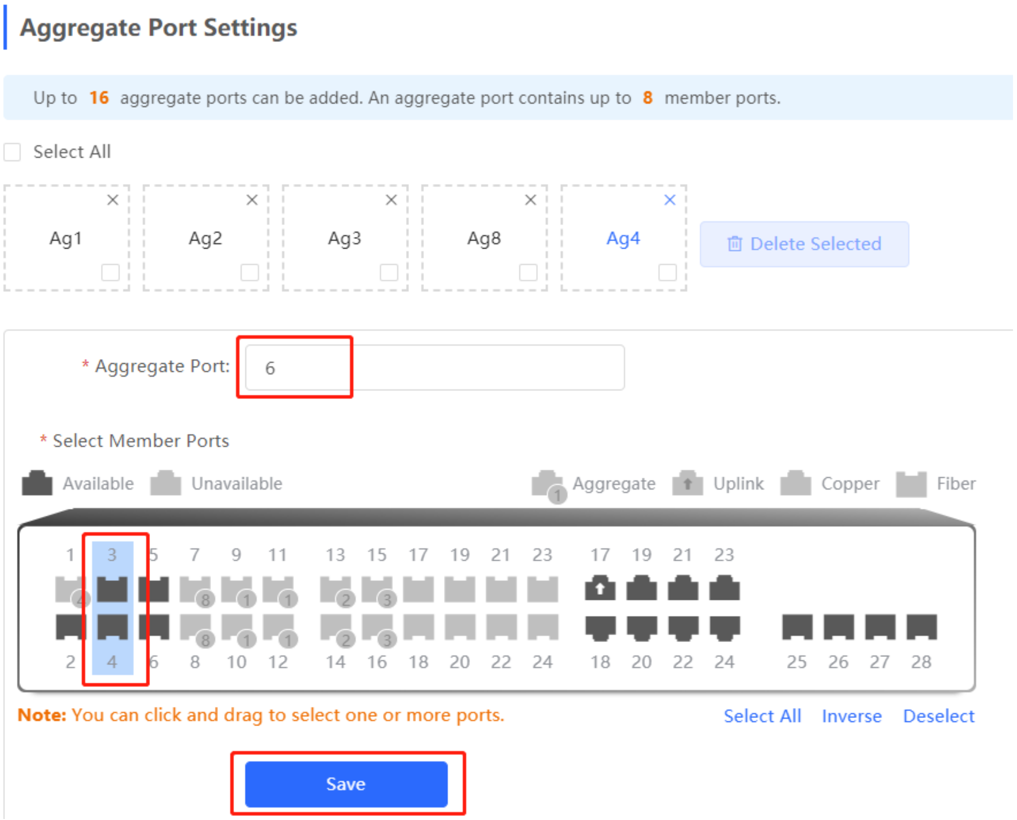
Choose **Local Device** > **Ports** > **Aggregate Ports** > **Aggregate Port Settings**.

1. Adding a Static Aggregate Port

Enter an aggregate port ID, select member ports (ports that have been added to an aggregate port cannot be selected), and click **Save**. The port panel displays a successfully added aggregate port.

Note

- An aggregate port contains a maximum of eight member ports.
- The attributes of aggregate ports must be the same, and copper ports and SFP ports cannot be aggregated.
- Dynamic aggregate ports do not support manual creation.



Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

* Aggregate Port: 6

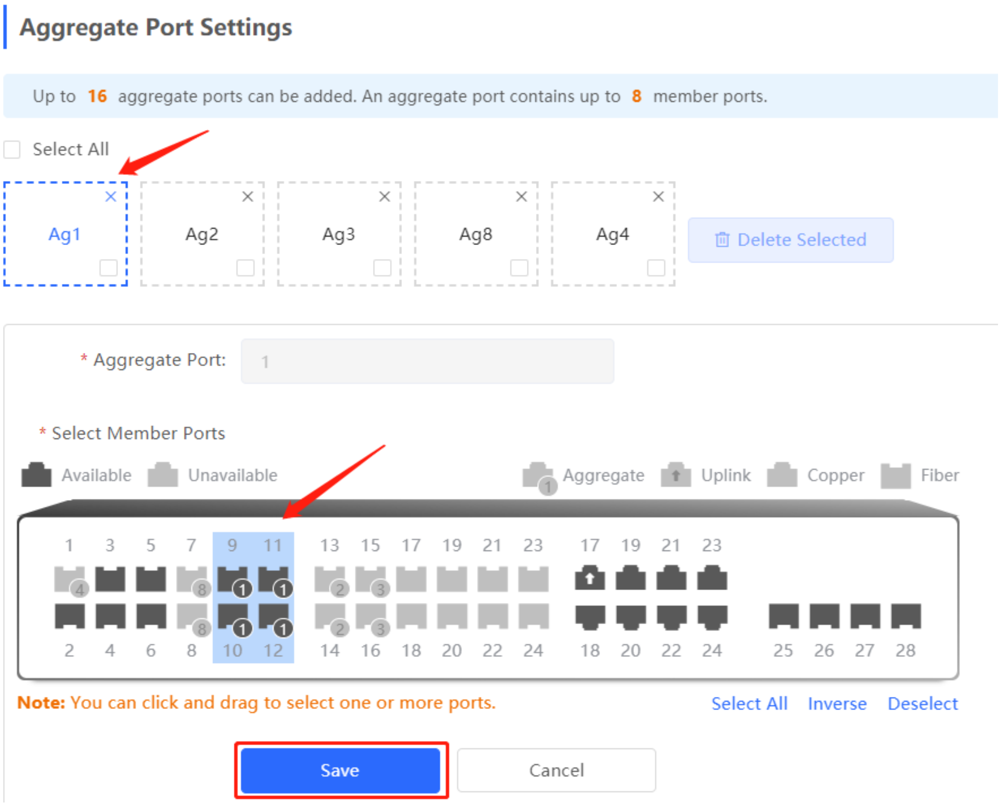
Note: You can click and drag to select one or more ports.

2. Modifying Member Ports of a Static Aggregate Port

Click an added static aggregate port. Member ports of the aggregate port will become selected. Click a port to deselect it; or select other ports to join the current aggregate port. Click **Save** to modify the member ports of the aggregate port.

Note

Dynamic aggregation ports do not support to modify member ports.



Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

□ Select All

* Aggregate Port: 1

* Select Member Ports

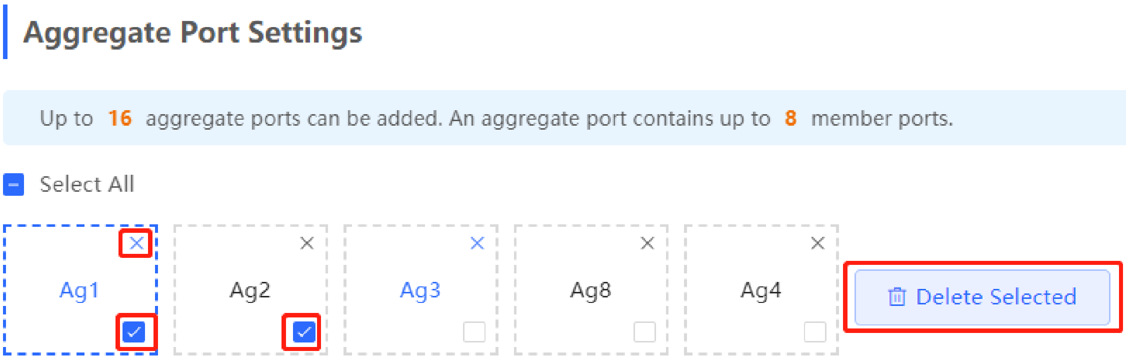
Note: You can click and drag to select one or more ports.

3. Deleting an Aggregate Port

Move the cursor over an aggregate port icon and click upper-right, or select the aggregate port to be deleted, and click **Delete Selected** to delete the selected aggregate port. After deleted, the corresponding ports become **available** on the port panel to set a new aggregate port.

Caution

After an aggregate port is deleted, its member ports are restored to the default settings and are disabled.



Aggregate Port Settings

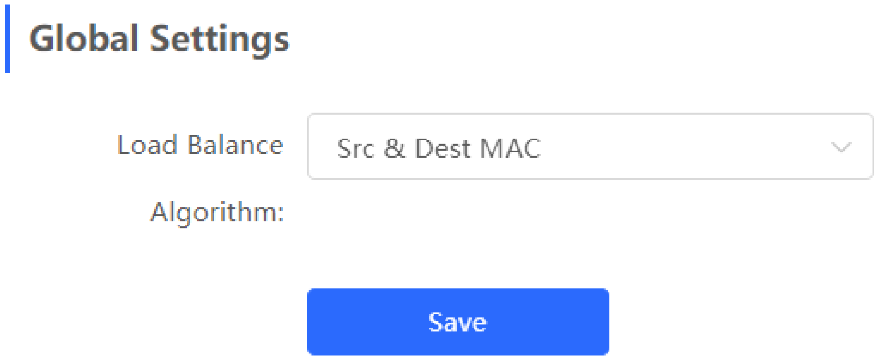
Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

Select All

12.3.4 Configuring a Load Balancing Mode

Choose **Local Device** > **Ports** > **Aggregate Port** > **Global Settings**.

Select **Load Balance Algorithm** and click **Save**. The Device 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.



Global Settings

Load Balance Algorithm: Src & Dest MAC

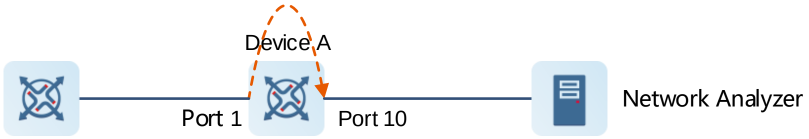
12.4 Port Mirroring

12.4.1 Overview

The switched port analyzer (SPAN) function is a function that copies packets of a specified port to another port that is connected to a network monitoring device, After port mirroring is set, the packets on the source port will be copied and forwarded to the destination port, and a packet analyzer is usually connected to the destination port to analyze the packet status of the source port, so as to monitor all incoming and outgoing packets on source ports.

As shown, by configuring port mirroring on Device A, the device copies the packets on Port 1 to Port 10. Although the network analysis device connected to Port 10 is not directly connected to Port 1, it can receive packets through Port 1. Therefore, the aim to monitor the data flow transmitted by Port 1 is realized.

Figure 12-1 Port Mirroring Principles Figure



The SPAN function not only realizes the data traffic analysis of suspicious network nodes or device ports, but also does not affect the data forwarding of the monitored device. It is mainly used in network monitoring and troubleshooting scenarios.

12.4.2 Procedure

Choose **Local Device** > **Ports** > **Port Mirroring**.

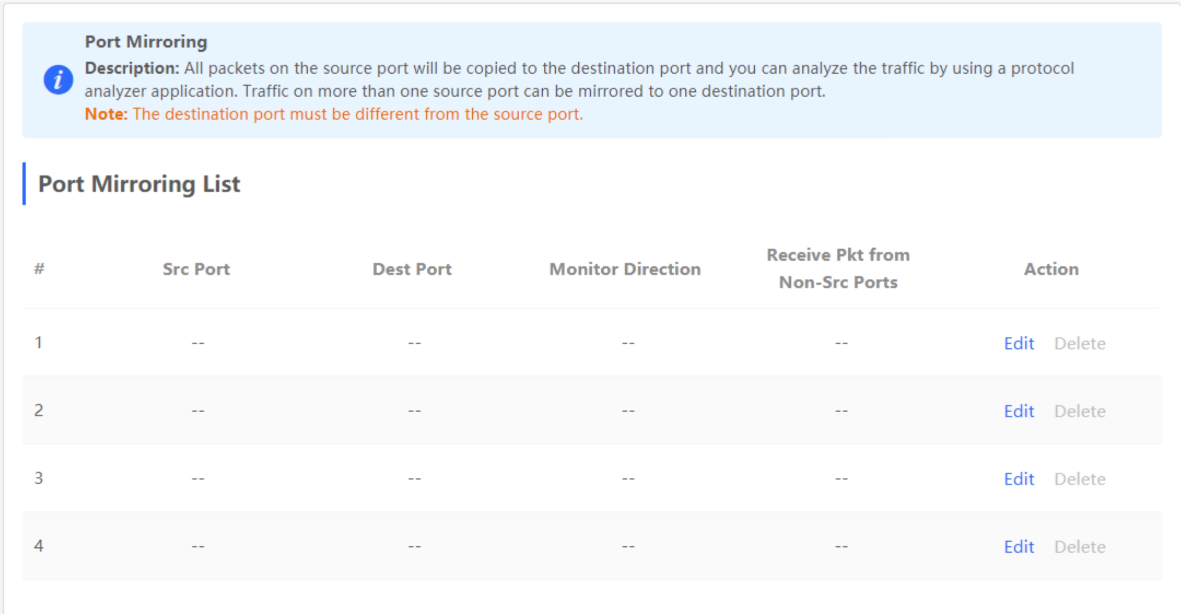
Click **Edit**, select the source port, destination port, monitor direction, and whether to receive packets from non-Src ports, and click **OK**. A maximum of four SPAN entries can be configured.

To delete the port mirroring configuration, click **Delete** in the corresponding **Action** column.

⚠ **Caution**

- You can select multiple source traffic monitoring ports but only one destination port. Moreover, the source traffic monitoring ports cannot contain the destination port.
- An aggregate port cannot be used as the destination port.

- A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.



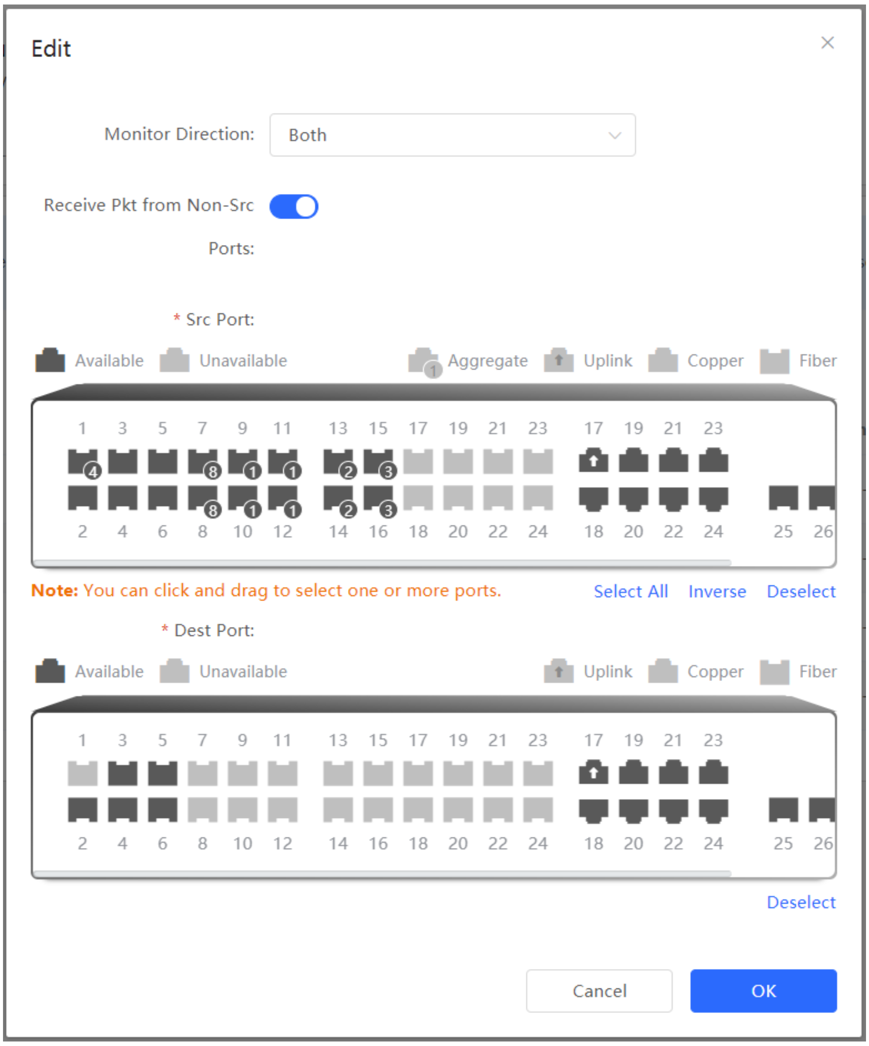
Port Mirroring

Description: All packets on the source port will be copied to the destination port and you can analyze the traffic by using a protocol analyzer application. Traffic on more than one source port can be mirrored to one destination port.

Note: The destination port must be different from the source port.

Port Mirroring List

#	Src Port	Dest Port	Monitor Direction	Receive Pkt from Non-Src Ports	Action
1	--	--	--	--	Edit Delete
2	--	--	--	--	Edit Delete
3	--	--	--	--	Edit Delete
4	--	--	--	--	Edit Delete



Edit

Monitor Direction: Both

Receive Pkt from Non-Src Ports: ●

* Src Port:

Note: You can click and drag to select one or more ports.

* Dest Port:

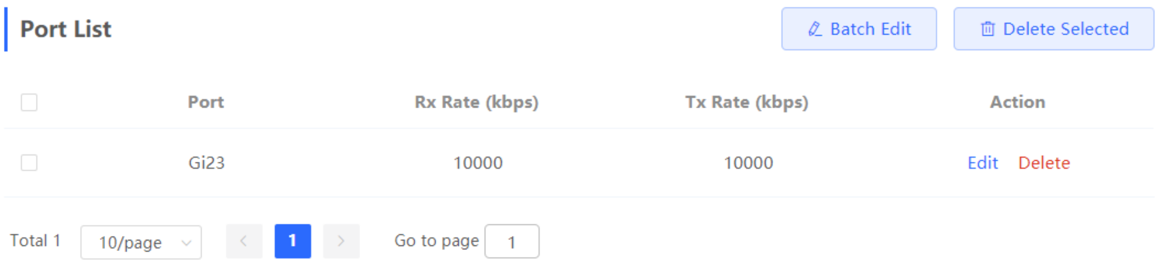
Table 4-4 Description of Port Mirroring Parameters

Parameter	**Description**	**Default Value**
Src Port	A source port is also called a monitored port. Data flows on the source port are monitored for network analysis or troubleshooting. Support selecting multiple source ports and mirroring multiple ports to one destination port	N/A
Dest Port	The destination port is also called the monitoring port, that is, the port connected to the monitoring device, and forwards the received packets from the source port to the monitoring device.	N/A
Monitor Direction	The type of packets (data flow direction) to be monitored by a source port. Both: All packets passing through the port, including incoming and outgoing packets Incoming: All packets received by a source port are copied to the destination port Outcoming: All packets transmitted by a source port are copied to the destination port	Both
Receive Pkt from Non-Src Ports	It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets. Enabled: While monitoring the packets of the source port, the packets of other non-Src ports are normally forwarded Disabled: Only monitor source port packets	Enable

12.5 Rate Limiting

Choose **Local Device** > **Ports** > **Rate Limiting**.

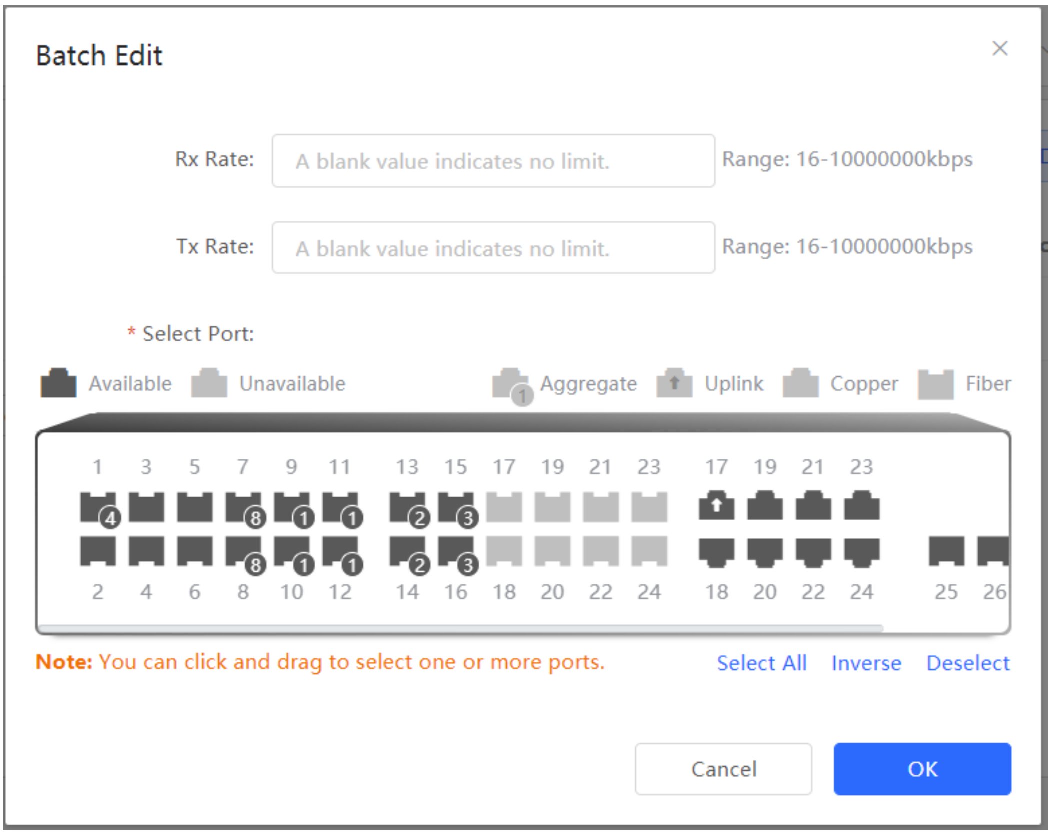
The **Rate Limiting** module allows you to configure traffic limits for ports, including rate limits for inbound and outbound direction of ports.



□	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
□	Gi23	10000	10000	Edit Delete

1. Rate Limiting Configuration

Click **Batch Edit**. In the displayed dialog box, select ports and enter the rate limits, and click **OK**. You must configure at least the ingress rate or egress rate. After the configuration is completed, it will be displayed in the list of port rate limiting rules.



Batch Edit

Rx Rate: A blank value indicates no limit. Range: 16-10000000kbps

Tx Rate: A blank value indicates no limit. Range: 16-10000000kbps

* Select Port:

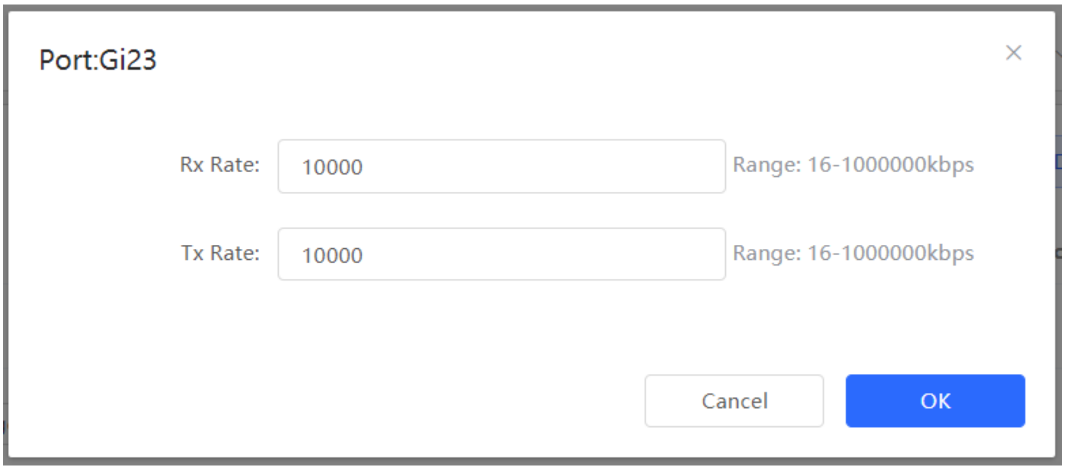
Note: You can click and drag to select one or more ports.

Table 4-5 Description of Rate Limiting Parameters

Parameter	Description	Default Value
Rx Rate	Max Rate at which packets are sent from a port to a switch, in kbps.	Not limited
Tx Rate	Max Rate at which packets are sent out of a switch through a port, in kbps.	Not limited

2. Changing Rate Limits of a Single Port

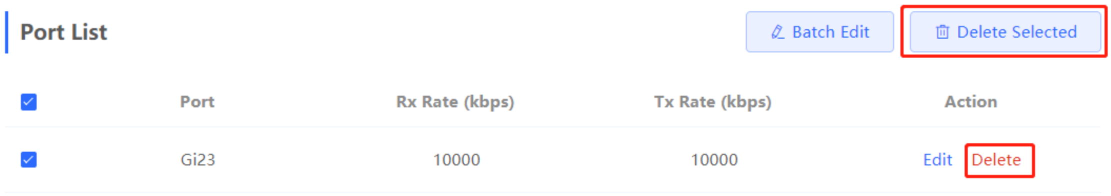
In the port list for which the rate limit has been set, click **Edit** on the corresponding port entry, enter the ingress rate and egress rate in the displayed dialog box, and click **OK**.



3. Deleting Rate Limiting

Batch configure: Select multiple records in **Port List**, click **Delete Selected** and click **OK** in the confirmation dialog box**.**

Configure one port: In **Port List**, click **Delete** on the corresponding port entry, and click **OK** in the confirmation dialog box.



☑	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
☑	Gi23	10000	10000	Edit Delete

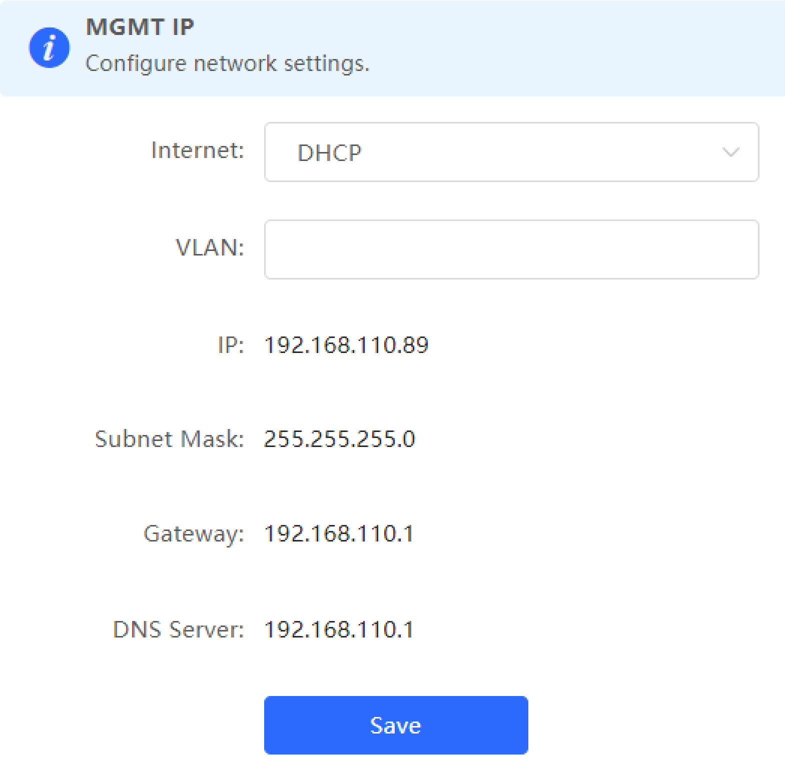
Note

- When configuring rate limits for a port, you must configure at least the ingress rate or egress rate.
- When the ingress rate or egress rate is not set, the port rate is not limited.

12.6 MGMT IP Configuration

Choose **Local Device** > **Ports** > **MGMT IP**.

The **MGMT IP** page allows you to configure the management IP address for the device. Users can configure and manage the device by accessing the management IP.


MGMT IP
Configure network settings.

Internet: DHCP

VLAN:

IP: 192.168.110.89

Subnet Mask: 255.255.255.0

Gateway: 192.168.110.1

DNS Server: 192.168.110.1

The device can be networked in two modes:

- DHCP: Uses a temporary IP address dynamically assigned by the upstream DHCP server for Internet access.
- Static IP: Uses a static IP address manually configured by users for Internet access.

If you select DHCP, the device obtains parameters from the DHCP Server. If Static IP is selected, you need to enter the management VLAN, IP address, subnet mask, default gateway IP address, and address of a DNS server. Click **Save** to make the configuration take effect.

Note

- If the management VLAN is null or not specified, VLAN 1 takes effect by default.
- The management VLAN must be selected from existing VLANs. If no VLAN is created, go to the VLAN list to add a VLAN (for details, see 11.5.2).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the Eweb management system.

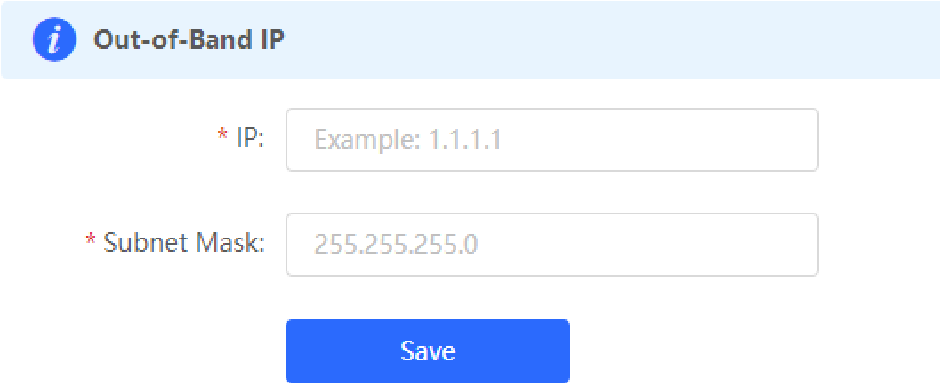
12.7 Out-of-Band IP Configuration

Caution

Only the RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series support this function.

Choose **Local Device** > **Ports** > **Out-of-Band IP**.

Set the MGMT management port IP of the chassis to centrally manage the modules in multiple slots of the device.



Out-of-Band IP

* IP: Example: 1.1.1.1

* Subnet Mask: 255.255.255.0

Note

No IP address is configured for the MGMT port by default. Currently, only a static IP address can be configured for the MGMT port but DHCP is not supported.

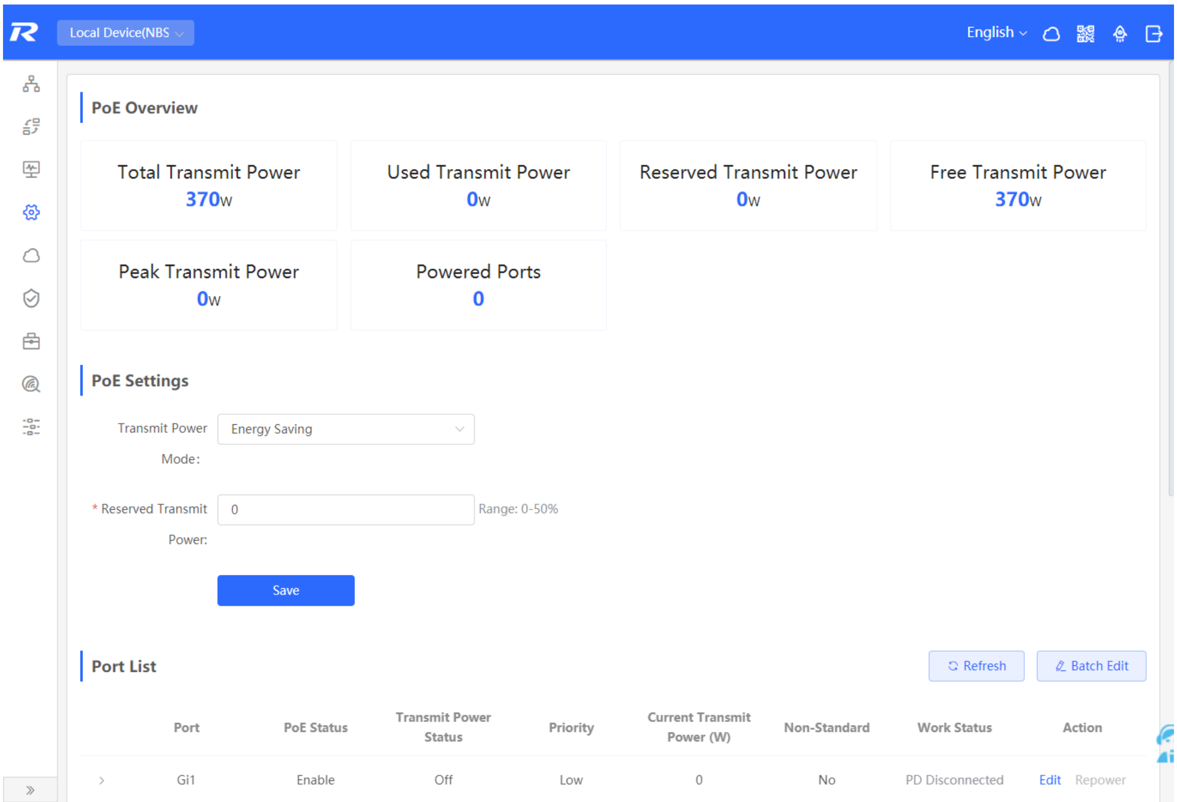
12.8 PoE Configuration

Caution

Only PoE switches (The device models are marked with **-P**) support this function.

Choose **Local Device** > **Ports** > **PoE**.

The device supplies power to PoE powered devices through ports. Users can view the current power supply status, and set the system power supply and port power supply policies respectively to achieve flexible power distribution.



PoE Overview

Total Transmit Power	Used Transmit Power	Reserved Transmit Power	Free Transmit Power
370w	0w	0w	370w
Peak Transmit Power	Powered Ports		
0w	0		

PoE Settings

Transmit Power Mode: Energy Saving

* Reserved Transmit Power: 0 Range: 0-50%

Port List

Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

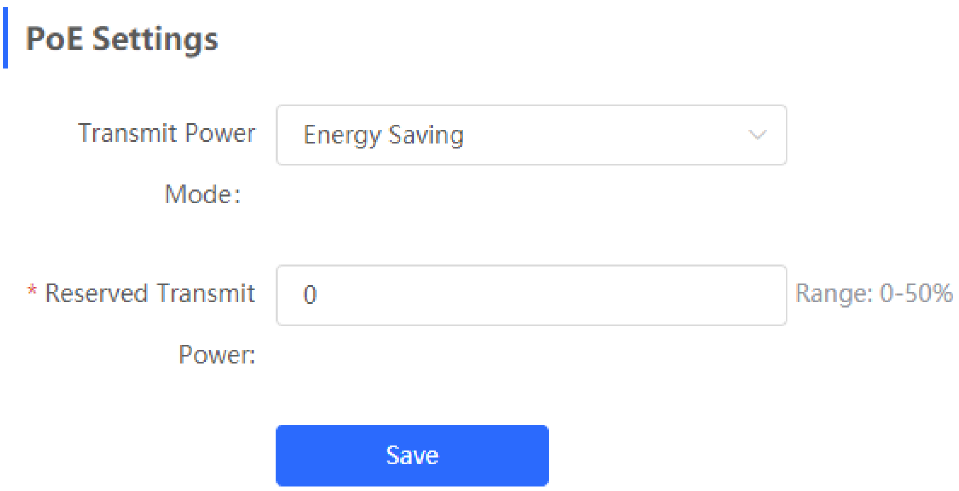
12.8.1 PoE Global Settings

Choose **Local Device** > **Ports** > **PoE** > **PoE Settings**.

PoE Transmit Power Mode refers to the way that a device allocates power to a connected PD (Powered Device). It supports Auto mode and Energy-saving mode.

In Auto mode, the system allocates power based on the classes of PDs detected on ports. The device allocates power to PD devices of Class 0~4 based on a fixed value: Class 0 is 15.4W, Class 1 is 4W, Class 2 is 7W, Class 3 is 15.4W, Class 4 Type 1 is 15.4W, and Class 4 Type 2 is 30W. In this mode, if the port is connected to a device of Class 3, even if the actual power consumption is only 11W, the PoE power supply device will allocate power to the port based on the power of 15.4W.

In energy-saving mode, the PoE device dynamically adjusts allocated power based on actual consumption of PDs. In this mode, in order to prevent the power supply of the port from fluctuating due to the fluctuation of the actual power consumption of the PD when the power is fully loaded, you can set the Reserved Transmit Power, and the reserved power will not be used for power supply, so as to ensure that the total power consumed by the current system does not exceed the limit of the PoE device. The size of the reserved power is expressed as a percentage of the total PoE power. The value ranges from 0 to 50.



PoE Settings

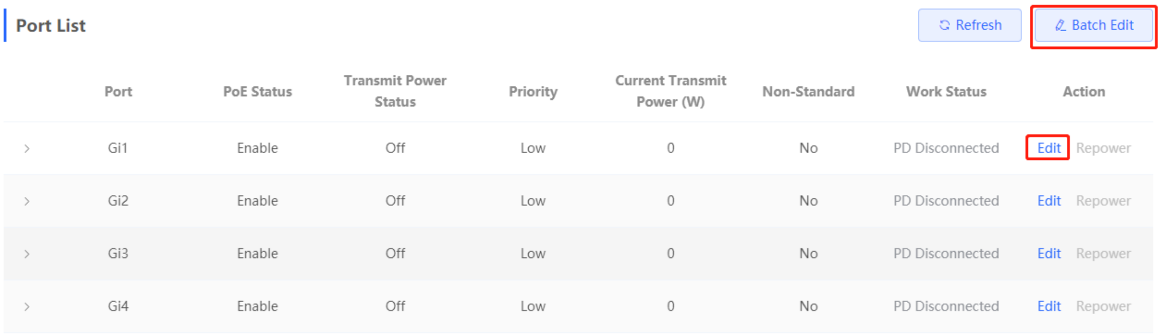
Transmit Power Mode: Energy Saving

* Reserved Transmit Power: 0 Range: 0-50%

12.8.2 Power Supply Configuration of Ports

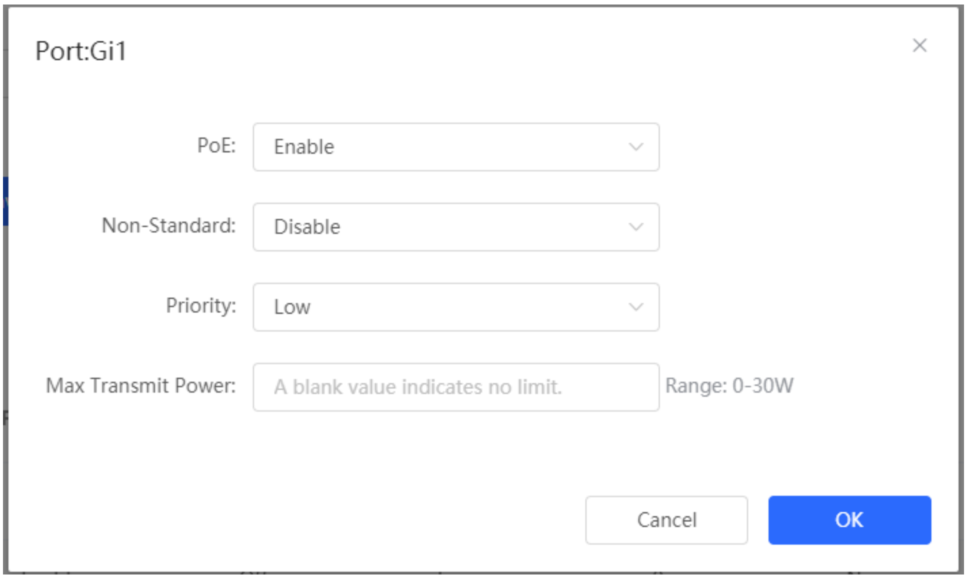
Choose **Local Device** > **Ports** > **PoE** > **Port List**.

Click **Edit** in the port entry or click **Batch Edit** to set the PoE power supply function of the port.



Port List

	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
›	Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Gi2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Gi3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Gi4	Enable	Off	Low	0	No	PD Disconnected	Edit Repower



Port:Gi1

PoE: Enable

Non-Standard: Disable

Priority: Low

Max Transmit Power: A blank value indicates no limit. Range: 0-30W

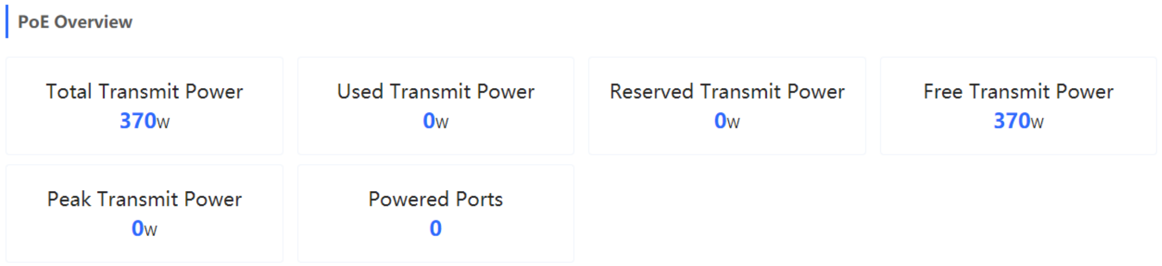
Table 4-6 Description of Parameters for Power Supply Configuration of Ports

Parameter	Description	Default Value
PoE	Whether to enable the power supply function on the ports	Enable
Non-Standard	By default, the device only supplies power to PDs that comply with the standard IEEE 802.3af and 802.3at protocols. In practical applications, there may be PDs that do not conform to the standard. After the non-standard mode is enabled, the device port can supply power to some non-standard PD devices.	Disable
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low In auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE device is insufficient, ports with low priorities are powered off first. Ports with the same priority are sorted by the port number. A smaller port number indicates a higher priority.	Low
Max Transmit Power	The maximum power that the port can transmit, ranging from 0 to 30, in watts (W). A blank value indicates no limit	Not limit

12.8.3 Displaying Global PoE Information

Choose **Local Device** > **Ports** > **PoE** > **PoE Overview**.

Displays the global power supply information of the PoE function, including the total system power, used power, reserved power, remaining available power, peak maximum power, and the number of ports currently powered.



PoE Overview

Total Transmit Power 370w

Used Transmit Power 0w

Reserved Transmit Power 0w

Free Transmit Power 370w

Peak Transmit Power 0w

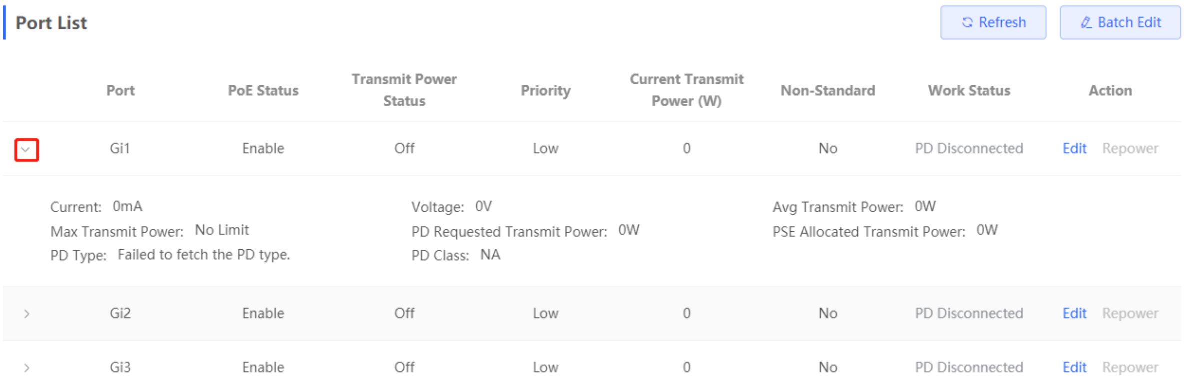
Powered Ports 0

12.8.4 Displaying the Port PoE Information

Choose **Local Device** > **PoE** > **Port List**.

The **Port List** displays the PoE configuration and status information of each port. Click to expand the detailed information.

When the PD device connected to the port needs to be restarted, for example, when the AP connected to the port is abnormal, you can click **Repower** to make the port power off briefly and then power on again to restart the device connected to the power supply port.



	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
⌄	Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Current: 0mA
Max Transmit Power: No Limit
PD Type: Failed to fetch the PD type.
Voltage: 0V
PD Requested Transmit Power: 0W
PD Class: NA
Avg Transmit Power: 0W
PSE Allocated Transmit Power: 0W

	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
›	Gi2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Gi3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Table 4-7 Description of Port Power Supply Info

Field	Description
Port	Device Port ID
PoE Status	Whether to enable the PoE function on the ports.
Transmit Power Status	Whether the port supplys power for Pds currently.
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low.
Current Transmit Power	Indicates the power output by the current port, in watts (W).
Non-Standard	Indicates whether the non-standard compatibility mode is enabled.
Work Status	Current work status of PoE ports.
Current	Indicates the present current of the port in milliamps (mA).
Voltage	Indicates the present current of the port in volts (V).
Avg Transmit Power	Indicates the current average power of the port, namely, the sampling average of current power after the port is powered on, in watts (W).
Max Transmit Power	The maximum output power of the port in watts (W).
PD Requested Transmit Power	The power requested by the PD to the PSE (Power Sourcing Equipment, power supply equipment), in watts (W).
PSE Allocated Transmit Power	Indicates the power allocated to a PD by PSE in watts (W).
PD Type	Information of PD type obtained through LLDP classification are divided into Type 1 and Type 2.
PD Class	The classification level of the PD connected to the port is divided into Class 0~4, based on the IEEE 802.3af/802.3at standard.

13 NBS Series L2 Multicast

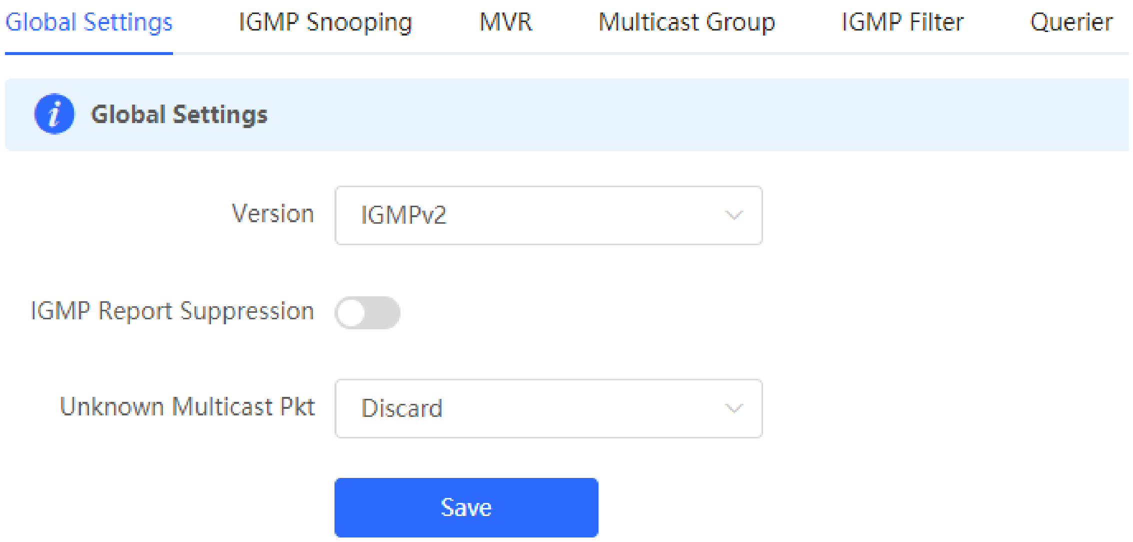
13.1 Multicast Overview

IP transmission methods are categorized into unicast, multicast, and broadcast. In IP multicast, an IP packet is sent from a source and forwarded to a specific group of receivers. Compared with unicast and broadcast, IP multicast saves bandwidth and reduces network loads. Therefore, IP multicast is applied to different network services that have high requirements for real timeliness, for example, Internet TV, distance education, live broadcast and multimedia conference.

13.2 Multicast Global Settings

Choose **Local Device** > **Multicast** > **Global Settings**.

Global Settings allow you to specify the version of the IGMP protocol, whether to enable report packet suppression, and the behavior for processing unknown multicast packets.



Version: IGMPv2

IGMP Report Suppression: ○

Unknown Multicast Pkt: Discard

Table 5-1 Description of Configuration Parameters of Global Multicast

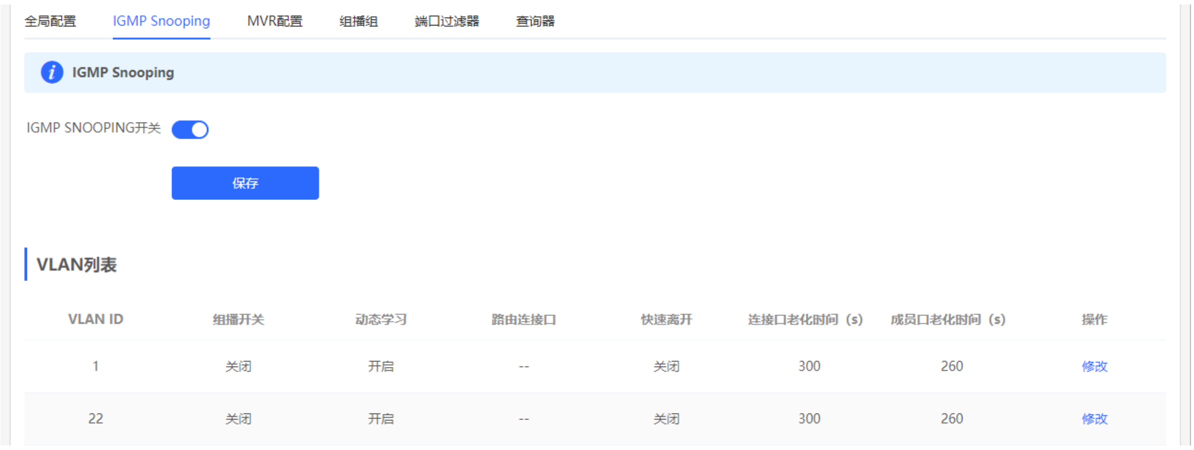
Parameter	Description	Default Value
Version	The Internet Group Management Protocol (IGMP) is a TCP/IP protocol that manages members in an IPv4 multicast group and runs on the multicast devices and hosts residing on the stub of the multicast network, creating and maintaining membership of the multicast group between the hosts and connected multicast devices. There are three versions of IGMP: IGMPv1, IGMPv2, IGMPv3. This parameter is used to set the highest version of IGMP packets that can be processed by Layer 2 multicast, and can be set to IGMPv2 or IGMPv3.	IGMPv2
IGMP Report Suppression	After this function is enabled, to reduce the number of packets in the network, save network bandwidth and ensure the performance of the IGMP multicast device, the switch forwards only one report packet to the multicast router if multiple downlink clients connected to the switch simultaneously send the report packet to demand the same multicast group.	Disable
Unknown Multicast Pkt	When both the global and VLAN multicast functions are enabled, the processing method for receiving unknown multicast packets can be set to Discard or Flood.	Discard

13.3 IGMP Snooping

13.3.1 Overview

The Internet Group Management Protocol (IGMP) snooping is an IP multicast snooping mechanism running on a VLAN to manage and control the forwarding of IP multicast traffic within the VLAN. It implements the L2 multicast function.

Generally, multicast packets need to pass through L2 switches, especially in some local area networks (LANs). When the Layer 2 switching device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2 switching device runs IGMP Snooping, the Layer 2 device can snoop the IGMP protocol packets of the user host and the upstream PIM multicast device. In this way, an Layer 2 multicast entry is established, and IP multicast packets are controlled to be sent only to group member receivers, preventing multicast data from being broadcast on the Layer 2 network.



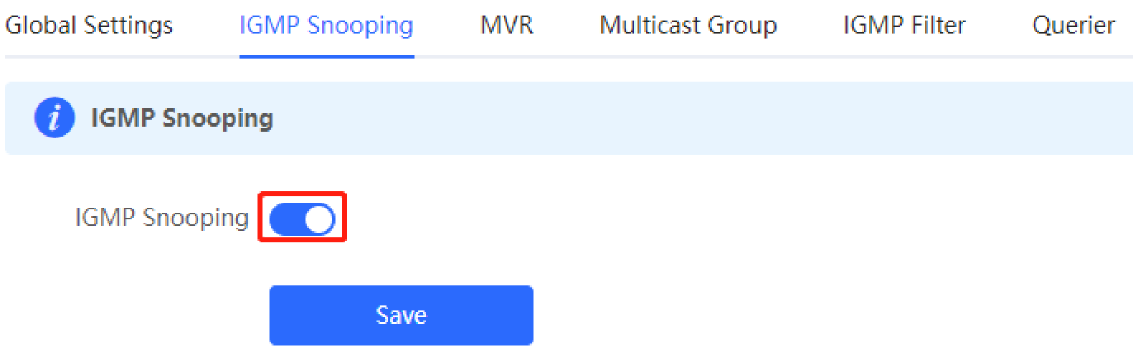
VLAN列表

VLAN ID	组播开关	动态学习	路由连接口	快速离开	连接口老化时间（s）	成员口老化时间（s）	操作
1	关闭	开启	--	关闭	300	260	修改
22	关闭	开启	--	关闭	300	260	修改

13.3.2 Enabling Global IGMP Snooping

Choose **Local Device** > **Multicast** > **IGMP Snooping**.

Turn on **IGMP Snooping** and click **Save**.



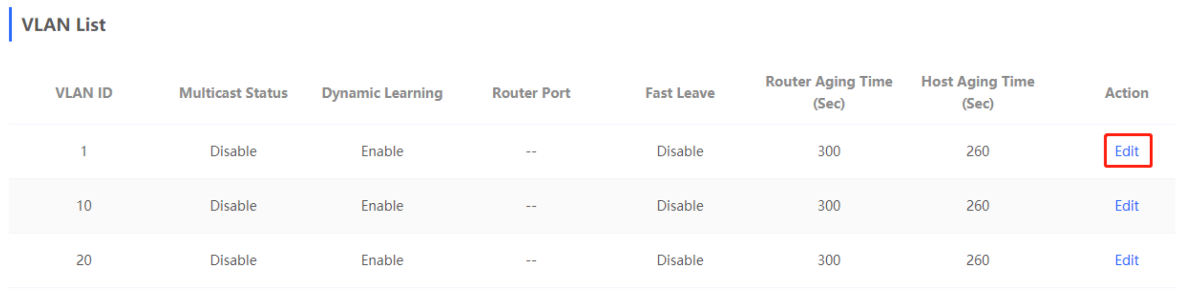
13.3.3 Configuring Protocol Packet Processing Parameters

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

Choose **Local Device** > **Multicast** > **IGMP Snooping**.

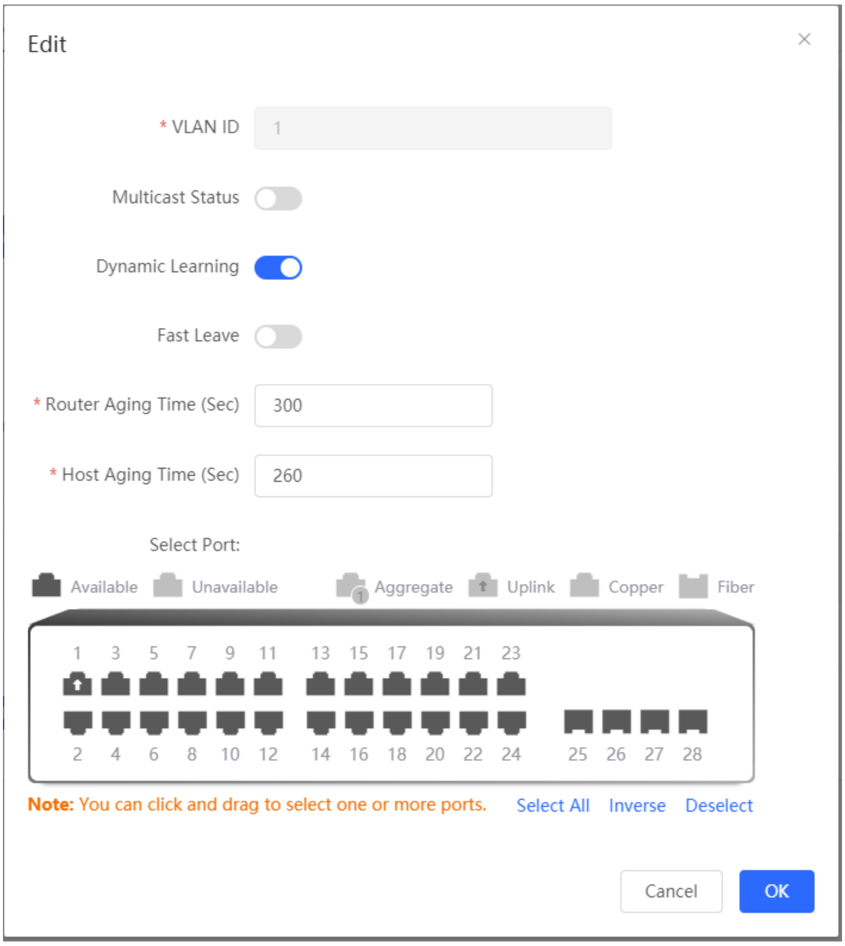
The IGMP Snooping function is implemented based on VLANs. Therefore, each VLAN corresponds to an IGMP Snooping setting entry. There are as many IGMP Snooping entries as VLANs on the device.

Click **Edit** in the VLAN entry. In the displayed dialog box enable/disable the VLAN multicast function, dynamic learning function, fast leave function and static route connection port , and set the router aging time and the host aging time, and click **OK**.



VLAN List

VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time (Sec)	Action
1	Disable	Enable	--	Disable	300	260	Edit
10	Disable	Enable	--	Disable	300	260	Edit
20	Disable	Enable	--	Disable	300	260	Edit



Edit

* VLAN ID: 1

Multicast Status: Off

Dynamic Learning: On

Fast Leave: Off

* Router Aging Time (Sec): 300

* Host Aging Time (Sec): 260

Select Port:

Note: You can click and drag to select one or more ports.

Table 5-2 Description of VLAN Configuration Parameters of IGMP Snooping

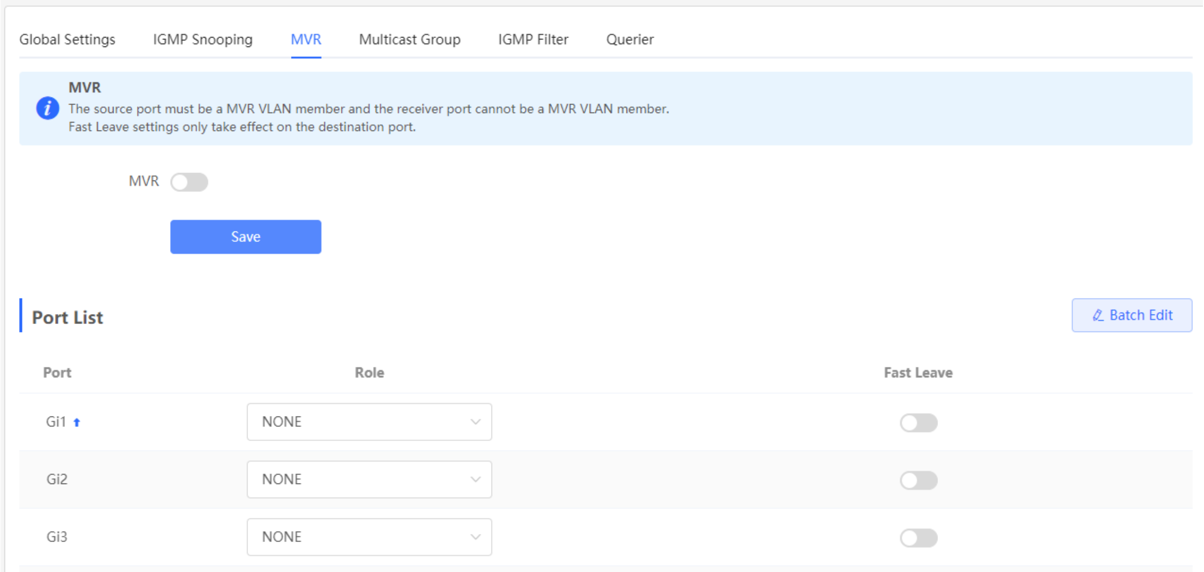
Parameter	Description	Default Value
Multicast Status	Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled.	Disable

Parameter	Description	Default Value
Dynamic Learning	The device running IGMP Snooping identifies the ports in the VLAN as router ports or member ports. The router port is the port on the Layer 2 multicast device that is connected to the Layer 3 multicast device, and the member port is the host port connected to the group on the Layer 2 multicast device. By snooping IGMP packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports.	Enable
Router Port	List of current multicast router ports includes dynamically learned routed ports (if Dynamic Learning function is enabled) and statically configured routed ports.	NA
Fast Leave	After it is enabled, when the port receives the Leave packets, it will immediately delete the port from the multicast group without waiting for the aging timeout. After that, when the device receives the corresponding specific group query packets and multicast data packets, the device will no longer forward it to the port. This function is applicable when only one host is connected to one port of the device, and is generally enabled on the access switch directly connected to the endpoint.	Disable
Router Aging Time (Sec)	Aging time of dynamically learned multicast router ports ranges from 30 to 3600, in seconds.	300 seconds
Host Aging Time (Sec)	Aging time of dynamically learned member ports of a multicast group, in seconds.	260 seconds
Select Port	In the displayed dialog box, select a port and set it as the static router port. When a port is configured as a static router port, the port will not age out	NA

13.4 Configuring MVR

13.4.1 Overview

IGMP snooping can forward multicast traffic only in the same VLAN. If multicast traffic needs to be forwarded to different VLANs, the multicast source must send multicast traffic to different VLANs. In order to save upstream bandwidth and reduce the burden of multicast sources, multicast VLAN register (MVR) comes into being. MVR can copy multicast traffic received from an MVR VLAN to the VLAN to which the user belongs and forward the traffic.


Global Settings IGMP Snooping MVR Multicast Group IGMP Filter Querier

MVR
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member.
Fast Leave settings only take effect on the destination port.

MVR

Save

Port List

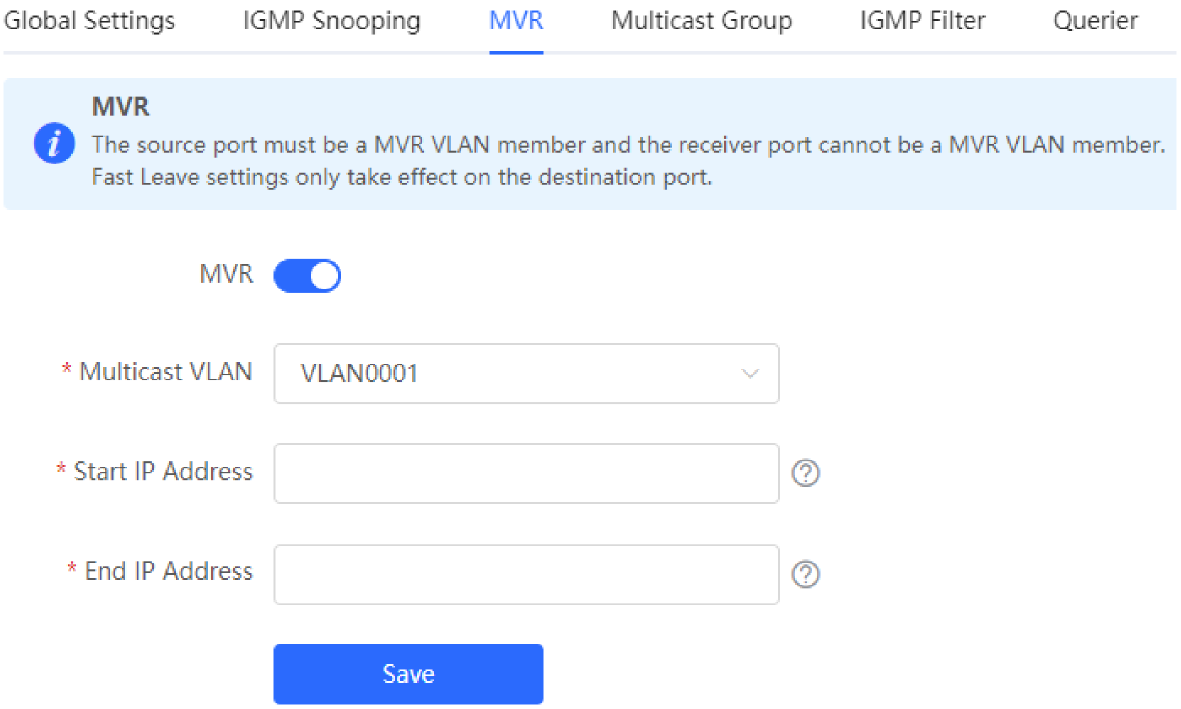
Batch Edit

Port	Role	Fast Leave
Gi1	NONE	
Gi2	NONE	
Gi3	NONE	

13.4.2 Configuring Global MVR Parameters

Choose **Local Device** > **L2 Multicast** > **MVR**.

Click to enable the MVR, select the MVR VLAN, set the multicast group supported by the VLAN, and click **Save**. Multiple multicast groups can be specified by entering the start and end multicast IP addresses.


Global Settings IGMP Snooping MVR Multicast Group IGMP Filter Querier

MVR
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member.
Fast Leave settings only take effect on the destination port.

MVR

* Multicast VLAN: VLAN0001

* Start IP Address

* End IP Address

Save

Table 5-3 Description of Configuring Global MVR Parameters

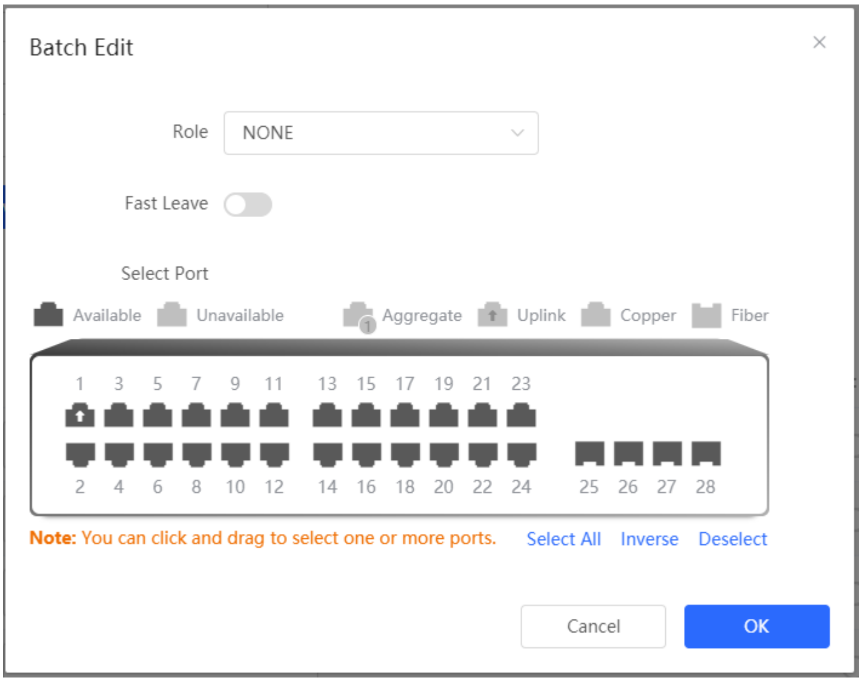
Parameter	Description	Default Value
MVR	Enables/Disables MVR globally	Disable

Parameter	Description	Default Value
Multicast VLAN	VLAN of a multicast source	1
Start IP Address	Learned or configured start multicast IP address of an MVR multicast group.	NA
End IP Address	Learned or configured end multicast IP address of an MVR multicast group.	NA

13.4.3 Configuring the MVR Ports

Choose **Local Device** > **L2 Multicast** > **MVR**.

Batch configure: Click **Batch Edit**, select the port role, the port to be set, and whether to enable the Fast Leave function on the port, and click **OK**.



Batch Edit

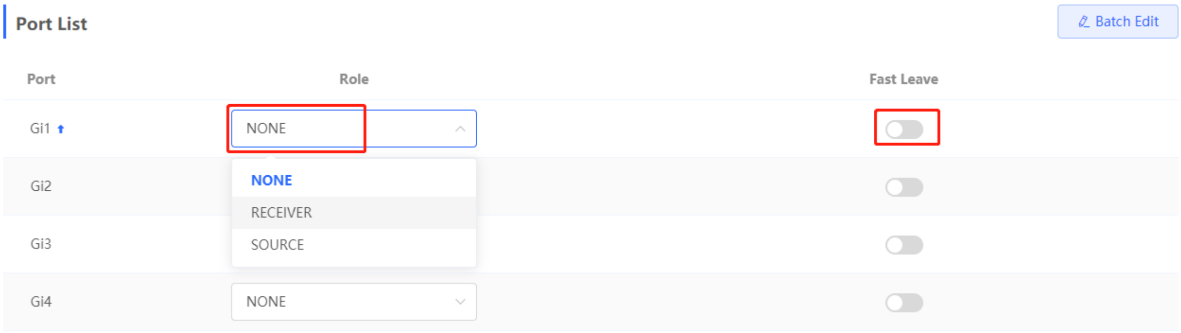
Role: NONE

Fast Leave

Select Port

Note: You can click and drag to select one or more ports.

Configure one port: Click the drop-down list box to select the MVR role type of the port. Click the switch in the **Fast Leave** column to set whether the port enables the fast leave function.



Port List

Port	Role	Fast Leave
Gi1	NONE	
Gi2		
Gi3		
Gi4	NONE	

Table 5-4 Description of MVR Configuration Parameters of Ports

Parameter	Description	Default Value
Role	**NONE**: Indicates that the MVR function is disabled. **SOURCE**: Indicates the source port that receives multicast data streams. **RECEIVER**: Indicates the receiver port connected to a client.	NONE
Fast Leave	Configures the fast leave function for a port. After the function is enabled, if the port receives the leave packet, it is directly deleted from the multicast group.	Disable

Note

- If a source port or a receiver port is configured, the source port must belong to the MVR VLAN and the receiver port must not belong to the MVR VLAN.
- The fast leave function takes effect only on the receiver port.

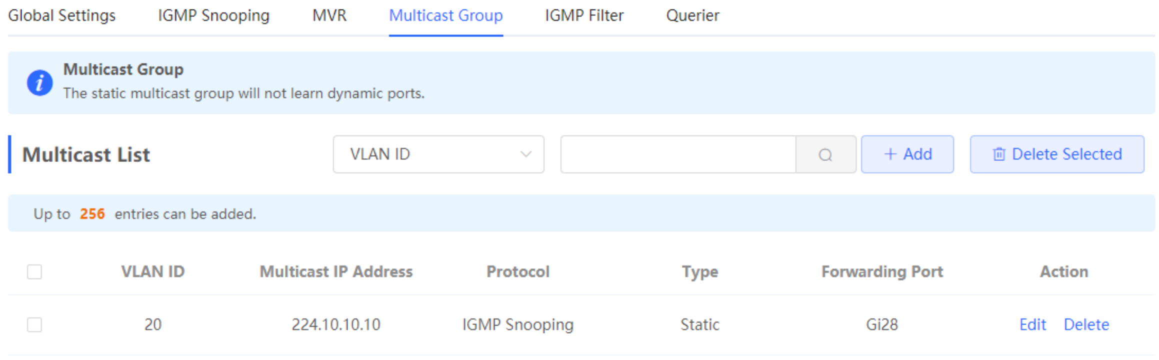
13.5 Configuring Multicast Group

Choose **Local Device** > **L2 Multicast** > **Multicast Group**.

A multicast group consists of the destination ports, to which multicast packets are to be sent. Multicast packets are sent to all ports in the multicast group.

You can view the **Multicast List** on the current page. The search box in the upper-right corner supports searching for multicast group entries based on VLAN IDs or multicast addresses.

Click **Add** to create a multicast group.



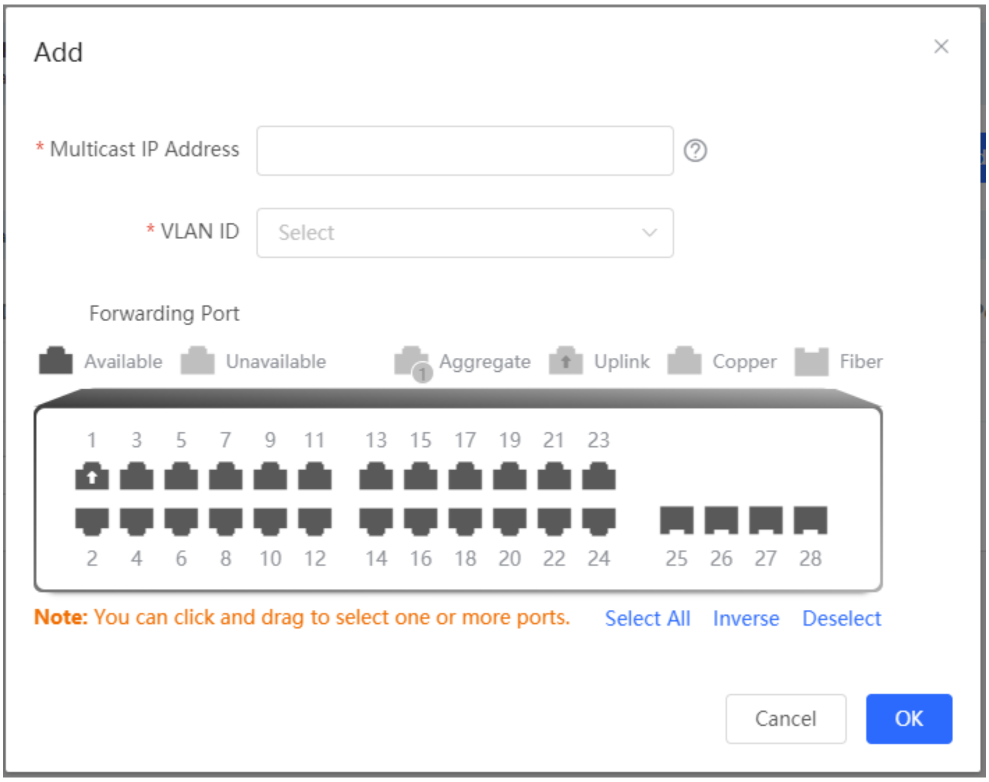
Multicast Group

The static multicast group will not learn dynamic ports.

Multicast List

Up to 256 entries can be added.

☐	VLAN ID	Multicast IP Address	Protocol	Type	Forwarding Port	Action
☐	20	224.10.10.10	IGMP Snooping	Static	Gi28	Edit Delete


Add

* Multicast IP Address

* VLAN ID: Select

Forwarding Port

Note: You can click and drag to select one or more ports.

Table 5-5 Description of Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	NA
Multicast IP Address	On-demand multicast IP address	NA
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	NA
Type	Multicast group generation mode can be statically configured or dynamically learned. In normal cases, a port can join a multicast group only after the port receives an IGMP Report packet from the multicast, that is, dynamically learned mode. If you manually add a port to a group, the port can be statically added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.	NA
Forwarding Port	List of ports that forward multicast traffic	NA

Note

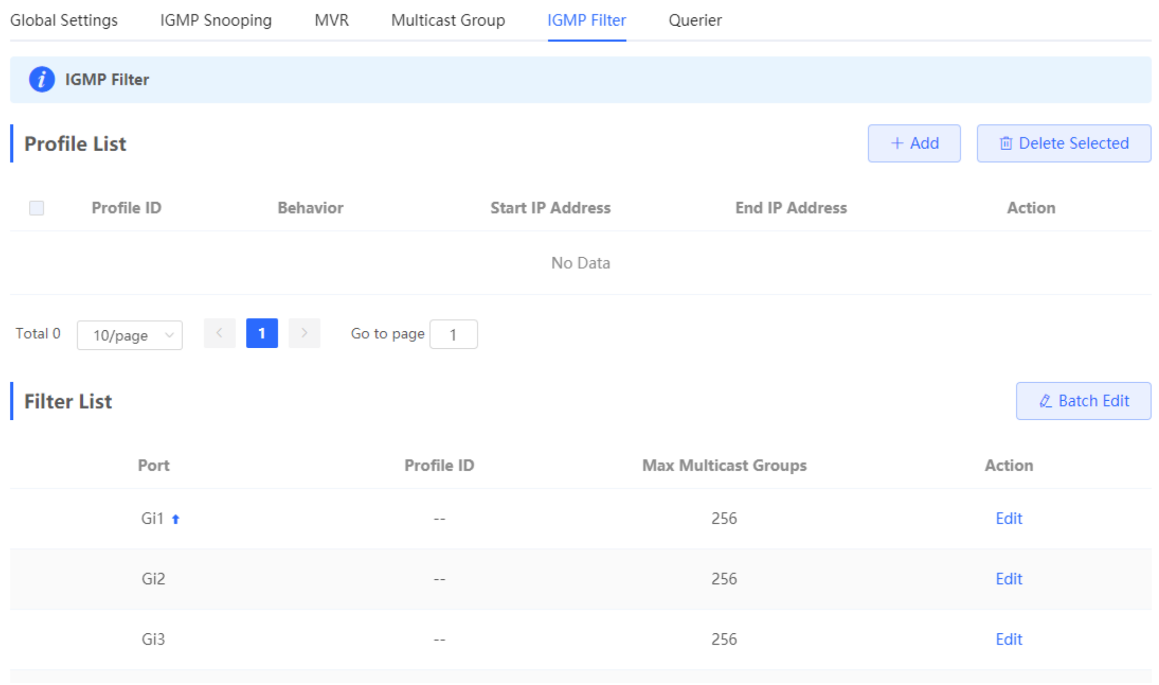
Static multicast groups cannot learn other dynamic forwarding ports.

13.6 Configuring a Port Filter

Choose **Local Device** > **L2 Multicast** > **IGMP Filter**.

Generally, the device running ports can join any multicast group. A port filter can configure a range of multicast groups that permit or deny user access, you can customize the multicast service scope for users to guarantee the interest of operators and prevent invalid multicast traffic.

There are 2 steps to configure the port filter: configure the profile and set a limit to the range of the port group address.



Profile List

□	Profile ID	Behavior	Start IP Address	End IP Address	Action
			No Data		

Filter List

Port	Profile ID	Max Multicast Groups	Action
Gi1	--	256	Edit
Gi2	--	256	Edit
Gi3	--	256	Edit

13.6.1 Configuring Profile

Choose **Local Device** > **L2 Multicast** > **IGMP Filter** > **Profile List**.

Click **Add** to create a **Profile**. A profile is used to define a range of multicast groups that permit or deny user access for reference by other functions.

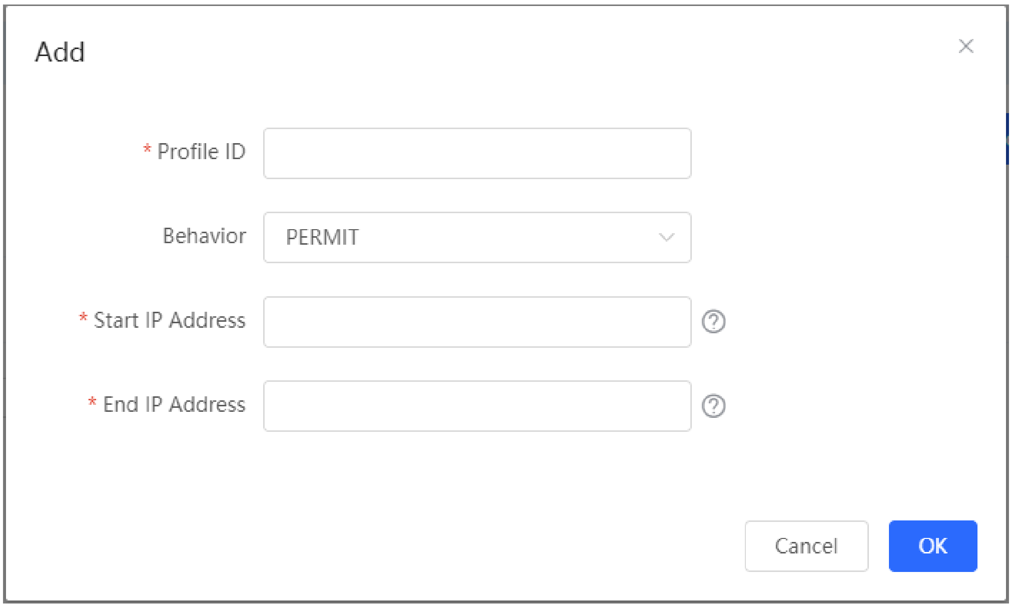


Table 5-6 Description of Profile Configuration Parameters

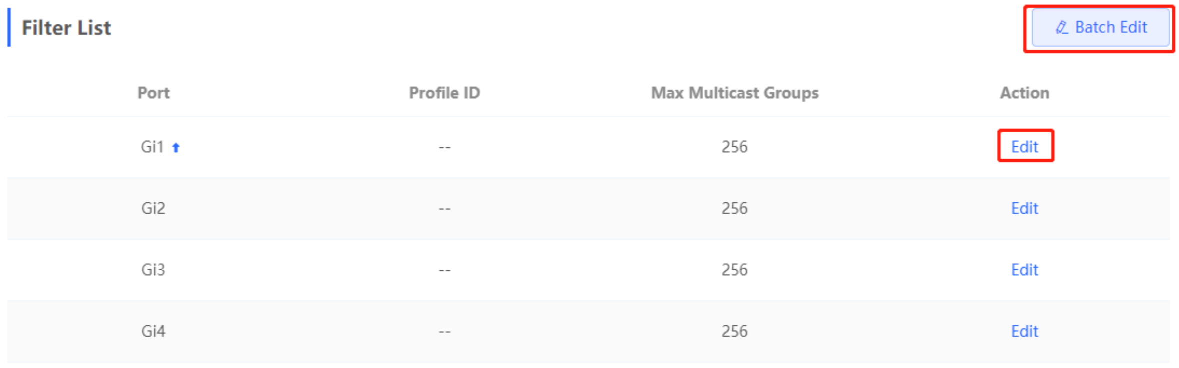
Parameter	Description	Default Value
Profile ID	Profile ID	NA
Behavior	DENY: Forbids demanding multicast IP addresses in a specified range. PERMIT: Only allows demanding multicast IP addresses in a specified range.	NA
Start IP Address	Start Multicast IP address of the range of multicast group addresses	NA
End IP Address	End Multicast IP address of the range of multicast group addresses	NA

13.6.2 Configuring a Range of Multicast Groups for a Profile

Choose **Local Device** > **L2 Multicast** > **IGMP Filter** > **Filter List**.

The port filter can cite a profile to define the range of multicast group addresses that can be or cannot be demanded by users on a port.

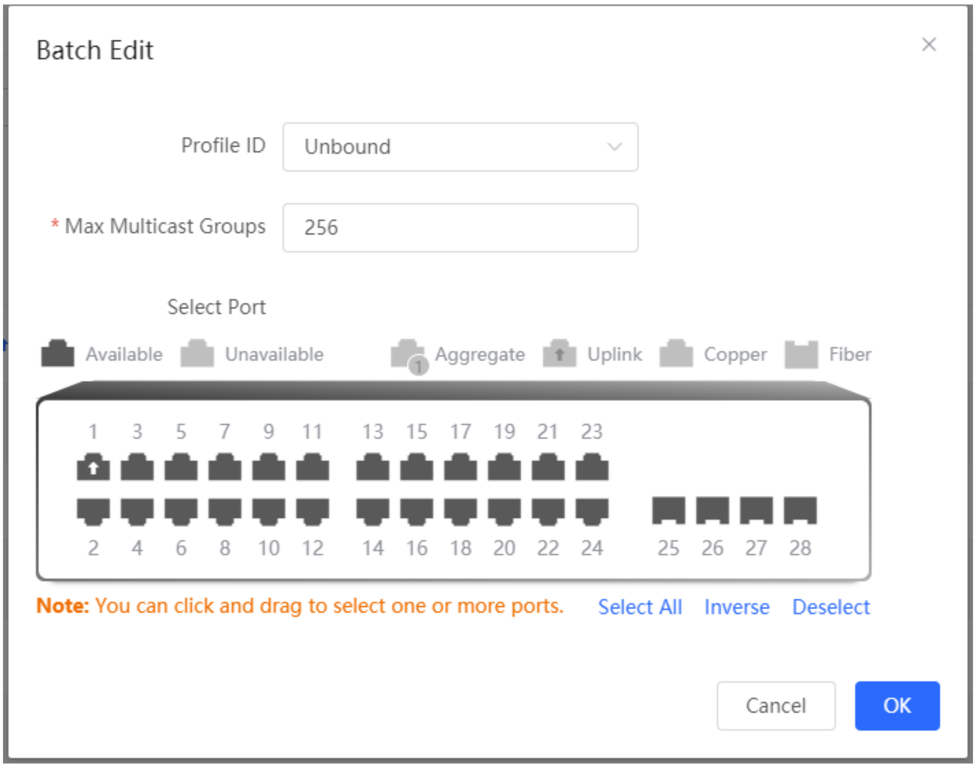
Click **Batch Edit**, or click **Edit** of a single port entry. In the displayed dialog box, select profile ID and enter the maximum number of multicast groups allowed by a port and click **OK**.



Filter List

Batch Edit

Port	Profile ID	Max Multicast Groups	Action
Gi1	--	256	Edit
Gi2	--	256	Edit
Gi3	--	256	Edit
Gi4	--	256	Edit



Batch Edit

Profile ID: Unbound

* Max Multicast Groups: 256

Select Port

Note: You can click and drag to select one or more ports.

Table 5-7 Description of Port Filter Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile that takes effect on a port. If it is not set, no profile rule is bound to the port.	NA
Max Multicast Groups	Maximum number of multicast groups that a port can join. If too much multicast traffic is requested concurrently, the multicast device will be severely burdened. Therefore, configuring the maximum number of multicast groups allowed for the port can guarantee the bandwidth.	256

13.7 Setting an IGMP Querier

13.7.1 Overview

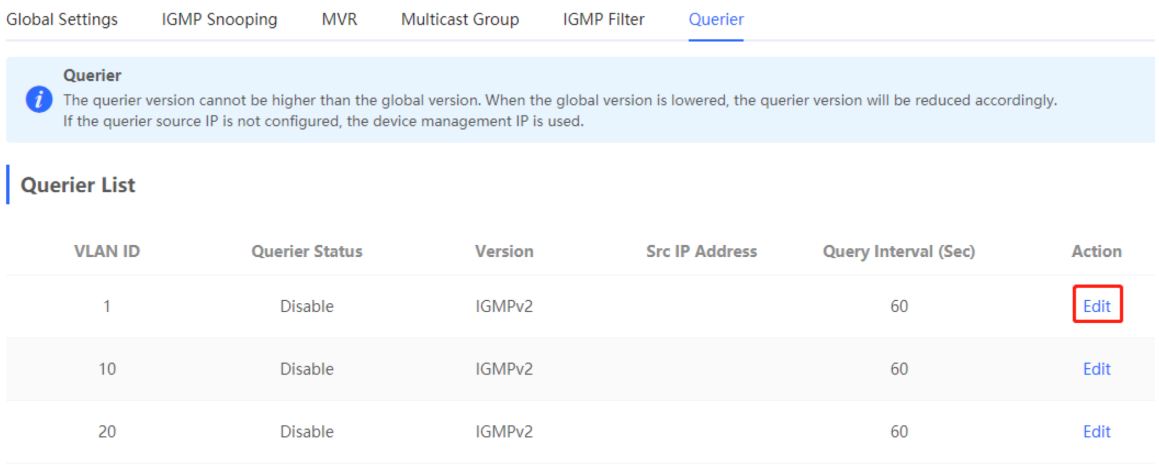
In a three-layer multicast network, the L3 multicast device serves as the querier and runs IGMP to maintain group membership. L2 multicast devices only need to listen to IGMP packets to establish and maintain forwarding entries and implement L2 multicasting. When a multicast source and user host are in the same L2 network, the query function is unavailable because the L2 device does not support IGMP. To resolve this problem, you can configure the IGMP snooping querier function on the L2 device so that the L2 device sends IGMP Query packets to user hosts on behalf of the L3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish L2 multicast forwarding entries.

13.7.2 Procedure

Choose **Local Device** > **L2 Multicast** > **Querier**.

One querier is set for each VLAN. The number of queriers is the same as that of device VLANs.

In **Querier List**, click **Edit** in the last **Action** column. In the displayed dialog box, select whether to enable the querier, set the querier version, querier source IP address, and packet query interval, and click **OK**.

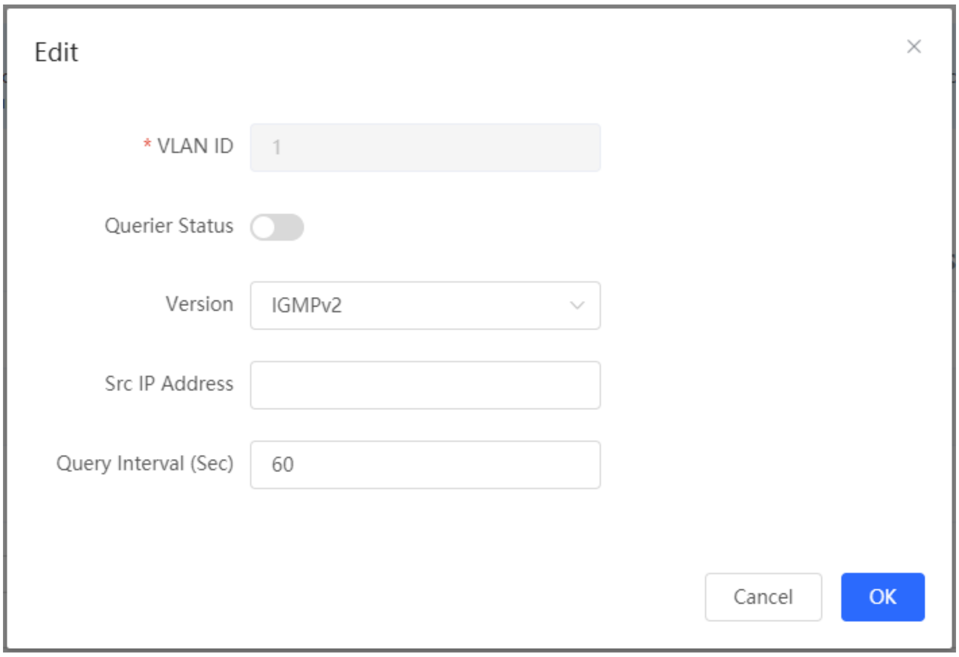


Querier

The querier version cannot be higher than the global version. When the global version is lowered, the querier version will be reduced accordingly.
If the querier source IP is not configured, the device management IP is used.

Querier List

VLAN ID	Querier Status	Version	Src IP Address	Query Interval (Sec)	Action
1	Disable	IGMPv2		60	Edit
10	Disable	IGMPv2		60	Edit
20	Disable	IGMPv2		60	Edit



* VLAN ID: 1

Querier Status: ○

Version: IGMPv2

Src IP Address:

Query Interval (Sec): 60

Table 5-8 Description of Querier Configuration Parameters

Parameter	Description	Default Value
Querier Status	Whether to enable or disable the VLAN querier function.	Disable
Version	IGMP Protocol version of query packets sent by the querier. It can be set to IGMPv2 or IGMPv3.	IGMPv2
Src IP Address	Source IP address carried in query packets sent by the querier.	NA
Query Interval (Sec)	Packet transmission interval, of which the value range is from 30 to 18000, in seconds.	60 seconds

Note

- The querier version cannot be higher than the global IGMP version. When the global IGMP version is lowered, the querier version is lowered accordingly.
- If no querier source IP is configured, the device management IP is used as the source IP address of the querier.

14 NBS Series L3 Management

Caution

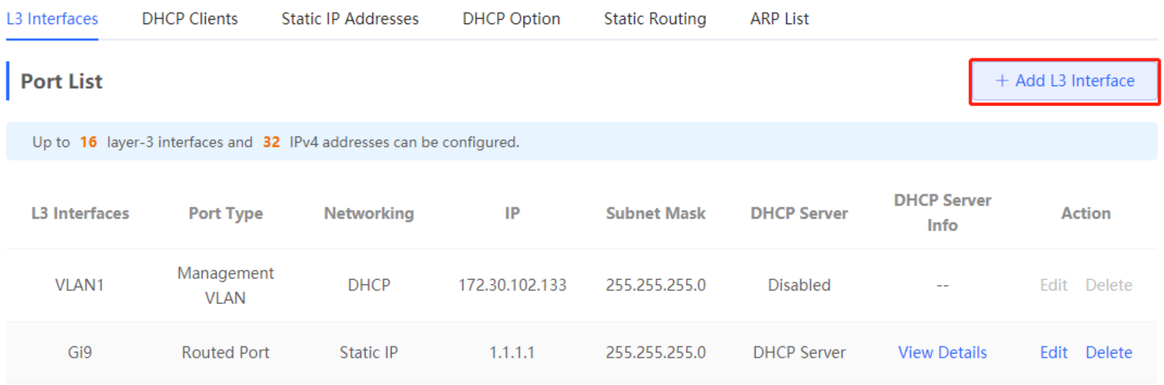
This section is applicable only to NBS Series Switches that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series Switches, RG-NBS3200 Series Switches, do not support the functions mentioned in this section.

14.1 Setting an L3 Interface

Choose **Local Device** > **L3 Interfaces** > **L3 Interfaces**.

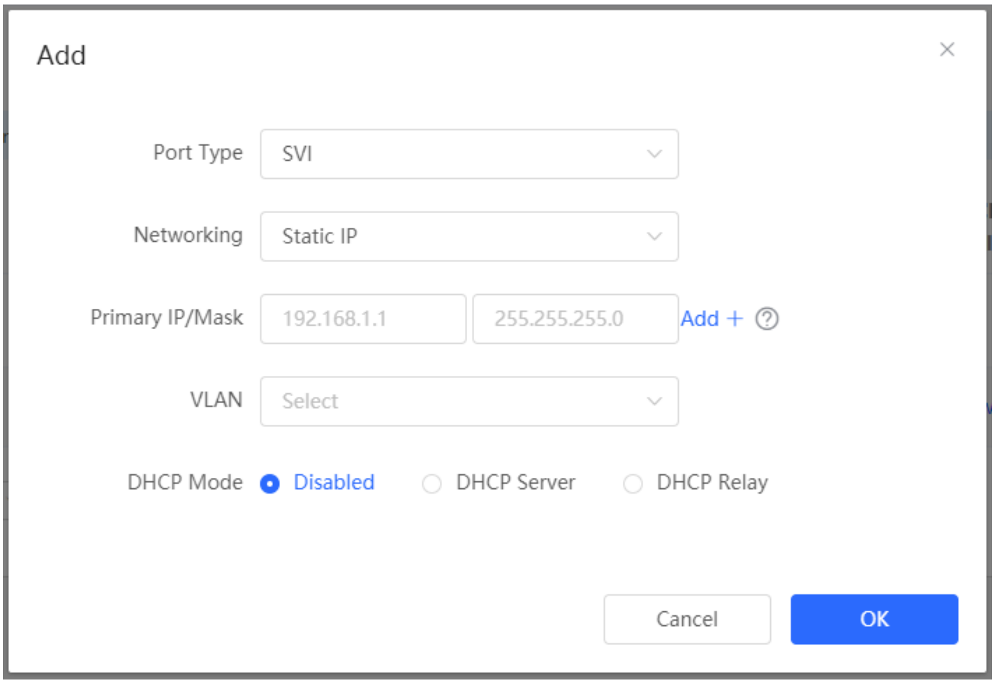
The port list displays various types of L3 interfaces on the device, including SVIs, Routed Ports, and L3 Aggregate Ports.

Click **Add L3 Interfaces** to set a new L3 Interface**.**



Up to 16 layer-3 interfaces and 32 IPv4 addresses can be configured.

L3 Interfaces	Port Type	Networking	IP	Subnet Mask	DHCP Server	DHCP Server Info	Action
VLAN1	Management VLAN	DHCP	172.30.102.133	255.255.255.0	Disabled	--	Edit Delete
Gi9	Routed Port	Static IP	1.1.1.1	255.255.255.0	DHCP Server	View Details	Edit Delete



Port Type: SVI

Networking: Static IP

Primary IP/Mask: 192.168.1.1 255.255.255.0

VLAN: Select

DHCP Mode ● Disabled ○ DHCP Server ○ DHCP Relay

Table 6-1 Description of Configuration Parameters of L3 Interfaces

Parameter	Description
Port Type	The type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port. For details, see Table 4-1
Networking	Specifies DHCP or static mode for a port to obtain the IP address.
VLAN	Specifies the VLAN, to which an SVI belongs.
IP/Mask	When Networking is set to Static IP, you need to manually enter the IP address and subnet mask.
Select Port	Select the device port to be configured.
Aggregate	Specifies the aggregate port ID, for example, Ag1, when an L3 aggregate port is created.
DHCP Mode	Select whether to enable the DHCP service on the L3 interface. Disabled: Indicates that the DHCP service is disabled. No IP address can be assigned to clients connected to the interface. DHCP Server: Indicates that the device functions as the DHCP server to assign IP addresses to downlink devices connected to the interface. You need to set the start IP address of an address pool, number of IP addresses that can be assigned, and address lease; for more information, see 6.2. DHCP Relay: Indicates that the device serves as a DHCP relay, obtains IP addresses from an external server, and assigns the IP addresses to downlink devices. The interface IP address and DHCP server IP address need to be configured. The interface IP address must be in the same network segment as the address pool of the DHCP server.
Excluded IP Address (Range)	When the device acts as a DHCP server, set the IP address in the address pool that is not used for assignment

Note

- VLAN 1 is the default SVI of the device. It can be neither modified nor deleted.
- The management VLAN is only displayed on the **L3 Interfaces** page but cannot be modified.To modify it, choose **Ports** > **MGMT IP**. For details, see 12.6 .
- The DHCP relay and DHCP server functions of an L3 interface are mutually exclusive and cannot be configured at the same time.
- Member ports of an L3 interface must be routed ports.

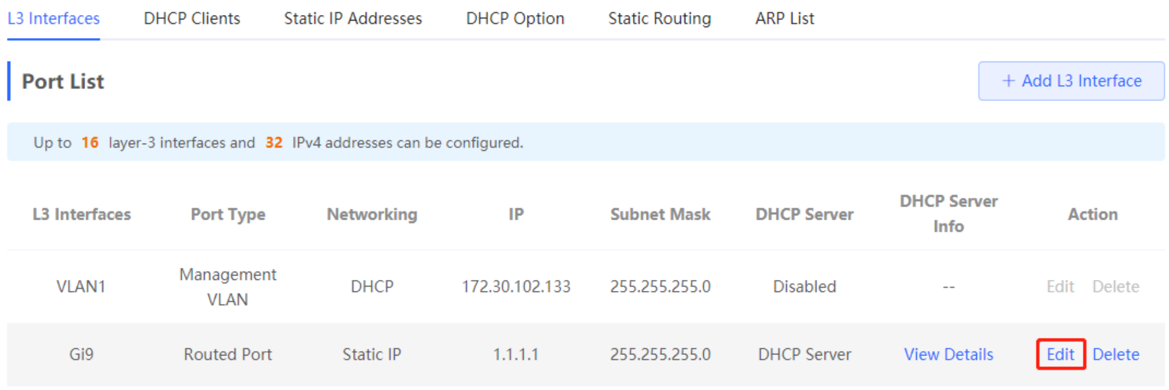
14.2 Configuring the DHCP Service

After the DHCP server function is enabled on the L3 interface, the device can assign IP addresses to downlink devices connected to the port.

14.2.1 Enable DHCP Services

Choose **Local Device** > **L3 Interfaces** > **L3 Interfaces**.

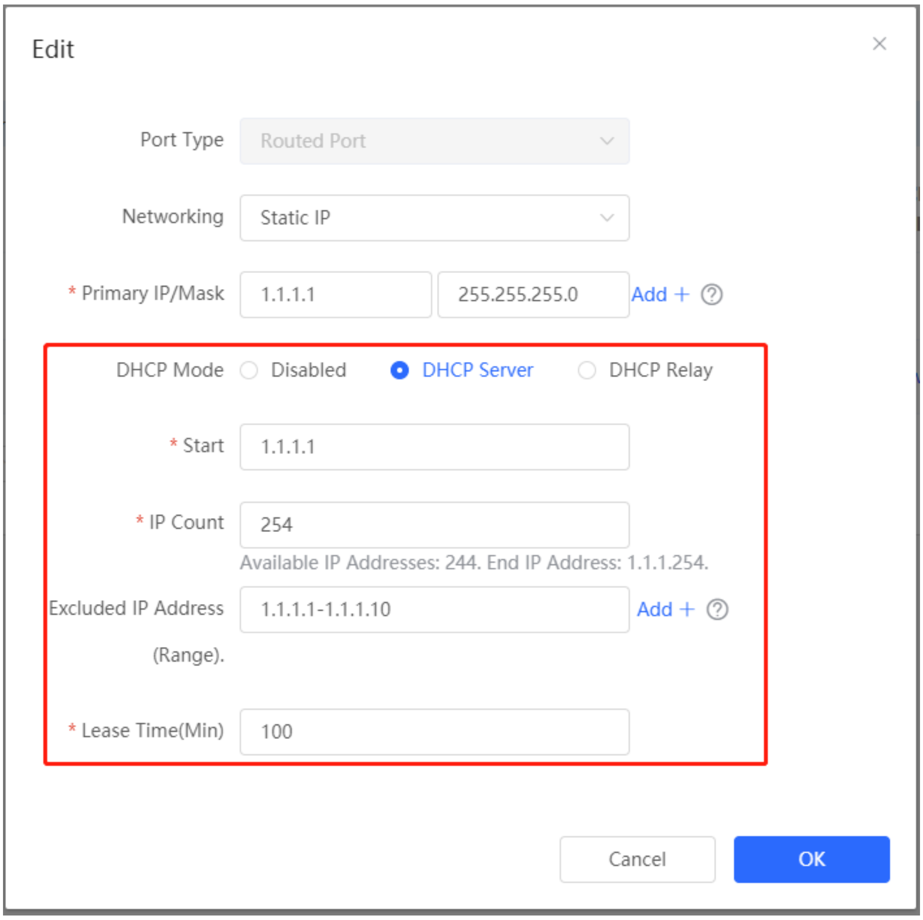
Click **Edit** on the designated port, or click **Add L3 Interface** to add a Layer 3 interface, select DHCP mode for local allocation, and enter the starting IP of the address pool, the number of allocated IPs, the excluded IP address range, and the address lease time.



Port List

Up to 16 layer-3 interfaces and 32 IPv4 addresses can be configured.

L3 Interfaces	Port Type	Networking	IP	Subnet Mask	DHCP Server	DHCP Server Info	Action
VLAN1	Management VLAN	DHCP	172.30.102.133	255.255.255.0	Disabled	--	Edit Delete
Gi9	Routed Port	Static IP	1.1.1.1	255.255.255.0	DHCP Server	View Details	Edit Delete



Edit

Port Type: Routed Port

Networking: Static IP

* Primary IP/Mask: 1.1.1.1 255.255.255.0

DHCP Mode: ○ Disabled ● DHCP Server ○ DHCP Relay

* Start: 1.1.1.1

* IP Count: 254

Available IP Addresses: 244. End IP Address: 1.1.1.254.

Excluded IP Address (Range).: 1.1.1.1-1.1.1.10

* Lease Time(Min): 100

Table 6-2 Description of DHCP Server Configuration Parameters

Parameter	Description
DHCP Mode	To choose DHCP server
Start	The DHCP server assigns the Start IP address automatically, which is the Start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up,

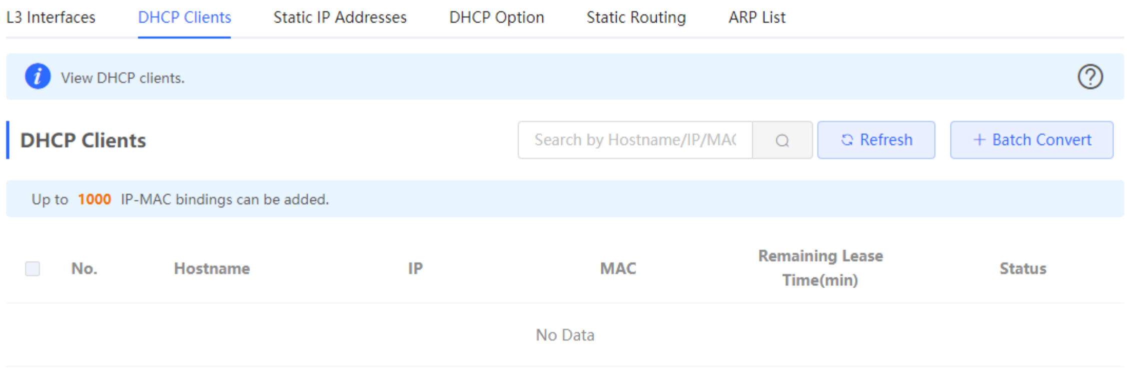
Parameter	Description
	no IP address can be obtained from the address pool.
IP Count	The number of IP addresses in the address pool
Excluded IP Address (Range)	IP addresses in the address pool that are not used for allocation, support inputting a single IP address or IP network segment, and add up to 20 address segments.
Lease Time(Min)	The lease of the address, in minutes.. Lease Time(Min): When a downlink client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease term expires. After the downlink client connection is restored, the client can request an IP address again

14.2.2 Viewing the DHCP Client

Choose **Local Device** > **L3 Interfaces** > **DHCP Clients**.

View the addresses automatically allocated to downlink clients after the L3 Interfaces enable DHCP services. You can find the client information based on the MAC address, IP address, or username.

Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Convert**. The dynamic address allocation relationship is added to the static address allocation list, so that the host can obtain the bound IP address for each connection. For details on how to view the static address allocation list, see 14.2.3 .



View DHCP clients.

DHCP Clients

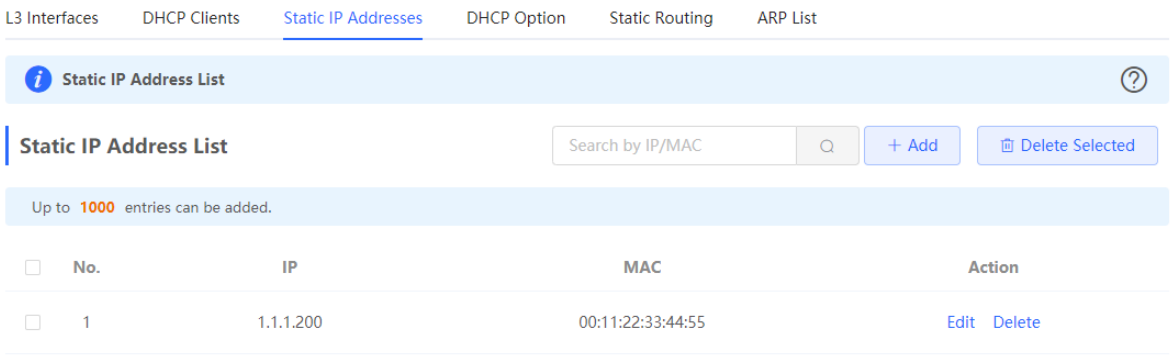
Up to 1000 IP-MAC bindings can be added.

□	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
No Data						

14.2.3 Configuring Static IP Addresses Allocation

Choose **Local Device** > **L3 Interfaces** > **Static IP Addresses**.

Displays the client entries which are converted into static addresses in the client list as well as manually added static address entries. The upper-right search box supports searching for corresponding entries based on the assigned IP address or the Device MAC Address

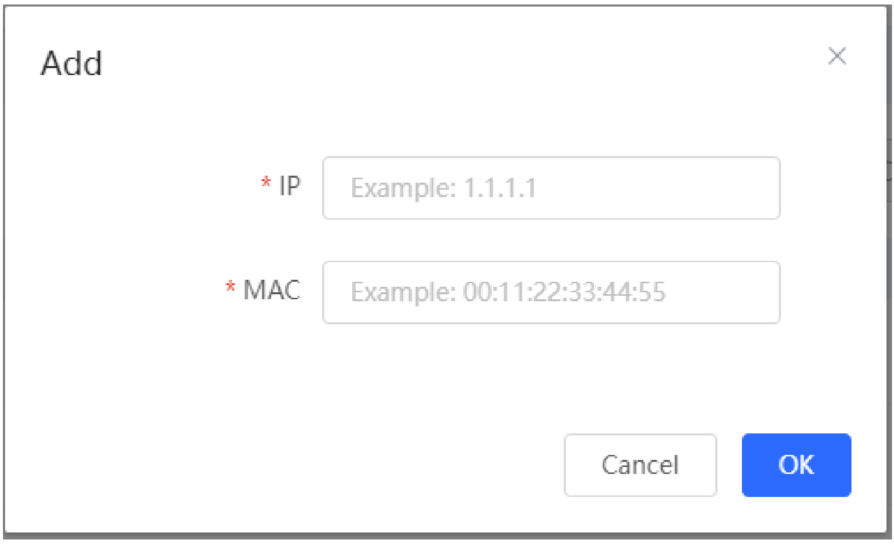


Static IP Address List

Up to 1000 entries can be added.

□	No.	IP	MAC	Action
□	1	1.1.1.200	00:11:22:33:44:55	Edit Delete

Click **Add**. In the displayed static IP address binding dialog box, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the corresponding downlink client connects to the network.



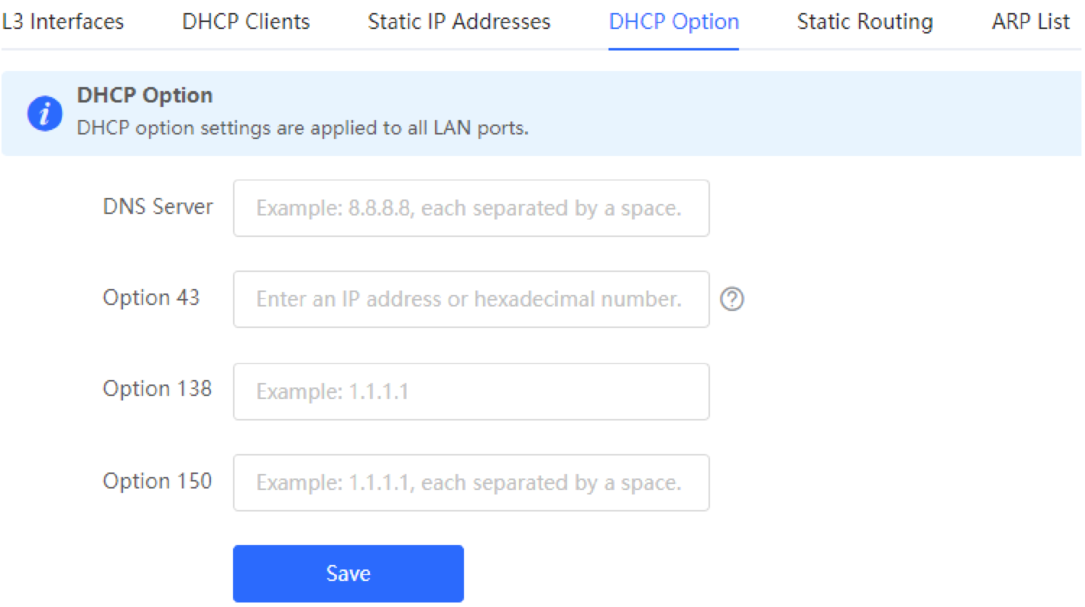
.

To delete a static address, select the static entry to be deleted in **Static IP Address List**, and click **Delete Selected**; or click **Delete** in the last **Action** column of the corresponding entry.

14.2.4 Configuring the DHCP Server Options

Choose **Local Device** > **L3 Interfaces** > **DHCP Option**.

The configuration delivered to the downlink devices is optional and takes effect globally when the L3 interface serves as the DHCP server.



DHCP Option
DHCP option settings are applied to all LAN ports.

DNS Server: Example: 8.8.8.8, each separated by a space.

Option 43: Enter an IP address or hexadecimal number.

Option 138: Example: 1.1.1.1

Option 150: Example: 1.1.1.1, each separated by a space.

Table 6-3 Description of the DHCP Server Options Configuration Parameters

Parameter	Description
DNS Server	DNS server address provided by an ISP. Multiple IP addresses can be entered and separated by spaces.
Option 43	When the AC (wireless controller) and the AP are not in the same LAN, the AP cannot discover the AC through broadcast after obtaining an IP address from the DHCP server. To enable the AP to discover the AC, you need to configure Option 43 carried in the DHCP response packet on the DHCP server.
Option 138	Enter the IP address of the AC. Similar to Option 43, when the AC and AP are not in the same LAN, you can configure Option 138 to enable the AP to obtain the IPv4 address of the AC.
Option 150	Enter the IP address of the TFTP server. Enter the IP address of the TFTP server to specify the TFTP server address assigned to the client. Multiple IP addresses can be entered and separated by spaces.

Note

DHCP options are optional configuration when the device functions as an L3 DHCP server. The configuration takes effect globally and does not need to be configured by default. If no DNS server address is specified, the DNS address assigned to a downlink port is the gateway IP address by default.

14.3 Configuring Static Routes

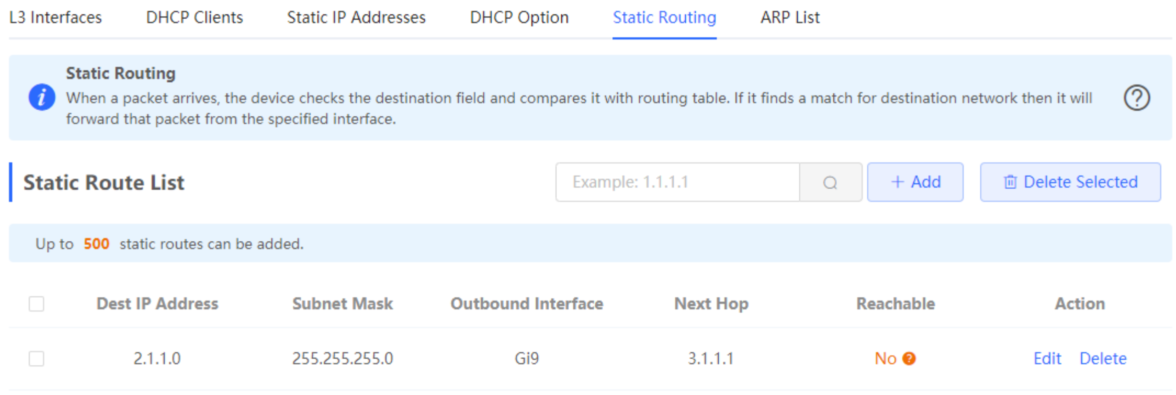
Choose **Local Device** > **L3 Interfaces** > **Static Routing**.

Static routes are manually configured by the user. When a data packet matches a static route, the packet will be forwarded according to the specified forwarding mode.

Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

Click **Add**. In the dialog box that appears, enter the destination address, subnet mask, outbound interface, and next-hop IP address to create a static route.



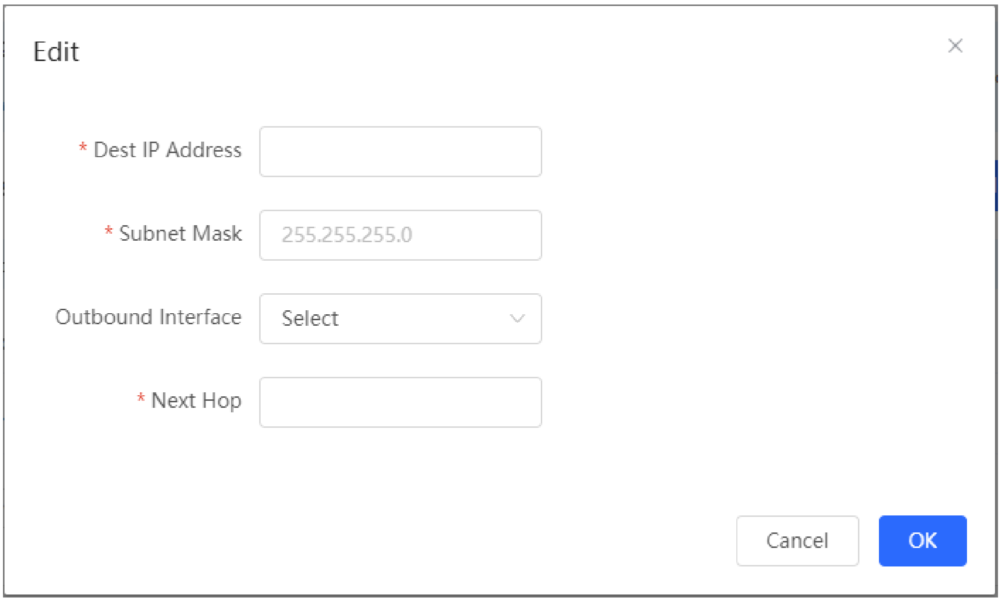
Static Routing

When a packet arrives, the device checks the destination field and compares it with routing table. If it finds a match for destination network then it will forward that packet from the specified interface.

Static Route List

Up to 500 static routes can be added.

□	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
□	2.1.1.0	255.255.255.0	Gi9	3.1.1.1	No	Edit Delete



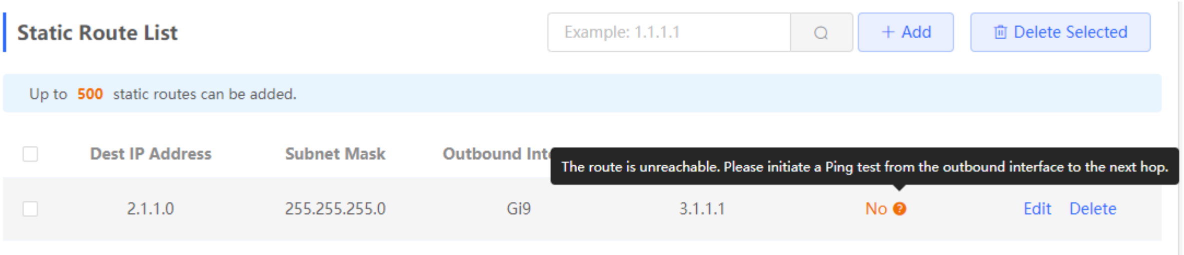
* Dest IP Address	
* Subnet Mask	255.255.255.0
Outbound Interface	Select
* Next Hop	

Table 6-4 Description of Static Routes Configuration Parameters

Parameter	Description
Dest IP Address	Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.

Parameter	Description
Outbound Interface	Specify the interface that forwards the data packet.
Next Hop	Specify the IP address of the next hop in the route for the data packet

After a static route is created, you can find the relevant route configuration and reachability status in the static route list. The **Reachable** parameter specifies whether the next hop is reachable, based on which you can determine whether the route takes effect. If the value is **No**, check whether the outbound interface in the current route can ping the next-hop address.



Static Route List

Up to 500 static routes can be added.

The route is unreachable. Please initiate a Ping test from the outbound interface to the next hop.

□	Dest IP Address	Subnet Mask	Outbound Int			
□	2.1.1.0	255.255.255.0	Gi9	3.1.1.1	No ❗	Edit Delete

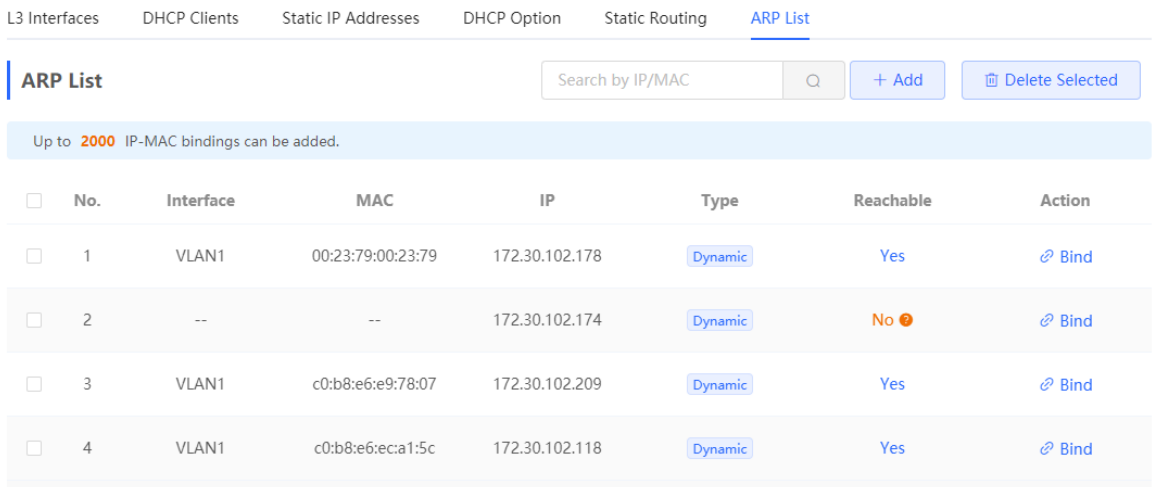
To delete or modify a static route, in **Static Route List**, you can click **Delete** or **Edit** in the last **Action** column; or select the static route entry to be deleted, click **Delete Selected** to delete multiple static route entries.

14.4 Configuring a Static ARP Entry

Choose **Local Device** > **L3 Interfaces** > **ARP List**.

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. Supports binding ARP mappings or manually specifying the IP address and MAC address mapping to prevent devices from learning wrong ARP entries and improve network security.

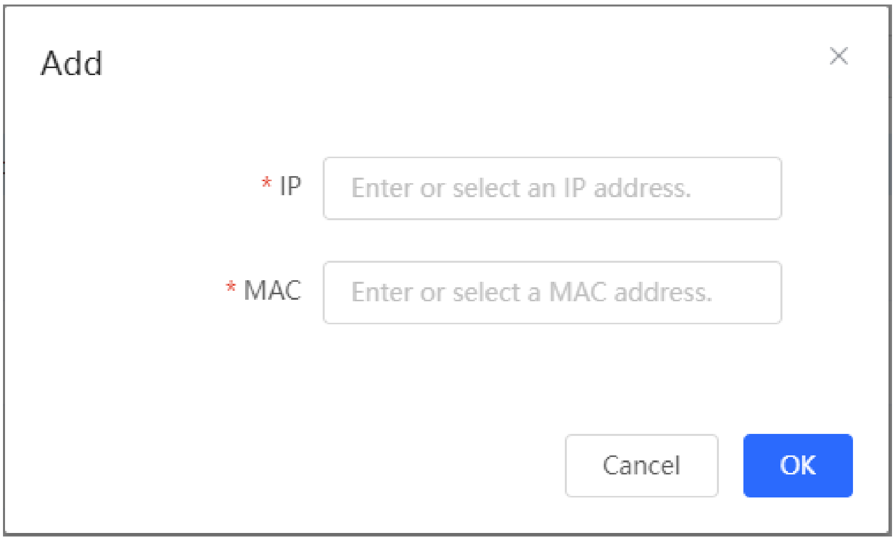
- To bind a dynamic ARP entry to a static entry: Select the ARP mapping entry dynamically obtained in the **ARP List**, and click **Bind** to complete the binding.
- To manually configure a static ARP entry: Click **Add**, enter the IP address and MAC address to be bound, and click **OK**.



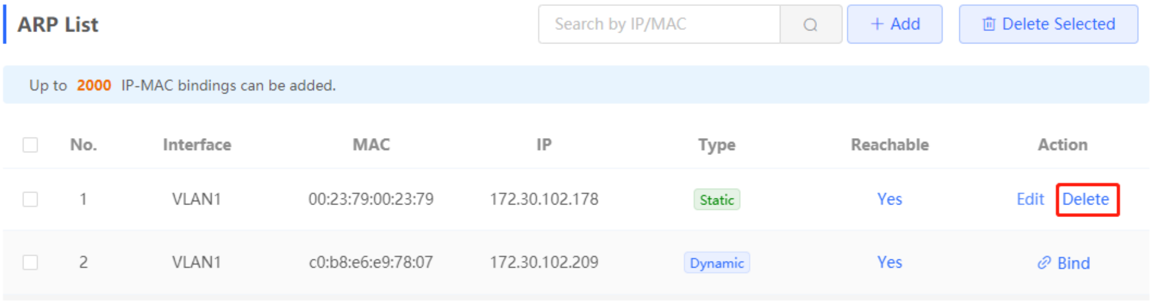
ARP List

Up to 2000 IP-MAC bindings can be added.

□	No.	Interface	MAC	IP	Type	Reachable	Action
□	1	VLAN1	00:23:79:00:23:79	172.30.102.178	Dynamic	Yes	Bind
□	2	--	--	172.30.102.174	Dynamic	No ❗	Bind
□	3	VLAN1	c0:b8:e6:e9:78:07	172.30.102.209	Dynamic	Yes	Bind
□	4	VLAN1	c0:b8:e6:ec:a1:5c	172.30.102.118	Dynamic	Yes	Bind


Add
* IP
Enter or select an IP address.
* MAC
Enter or select a MAC address.
Cancel
OK

To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.



Up to 2000 IP-MAC bindings can be added.

□	No.	Interface	MAC	IP	Type	Reachable	Action
□	1	VLAN1	00:23:79:00:23:79	172.30.102.178	Static	Yes	Edit Delete
□	2	VLAN1	c0:b8:e6:e9:78:07	172.30.102.209	Dynamic	Yes	Bind

15 NBS Series Security

15.1 DHCP Snooping

15.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server. DHCP snooping records generated user data entries to serve security applications such as IP Source Guard.

15.1.2 Standalone Device Configuration

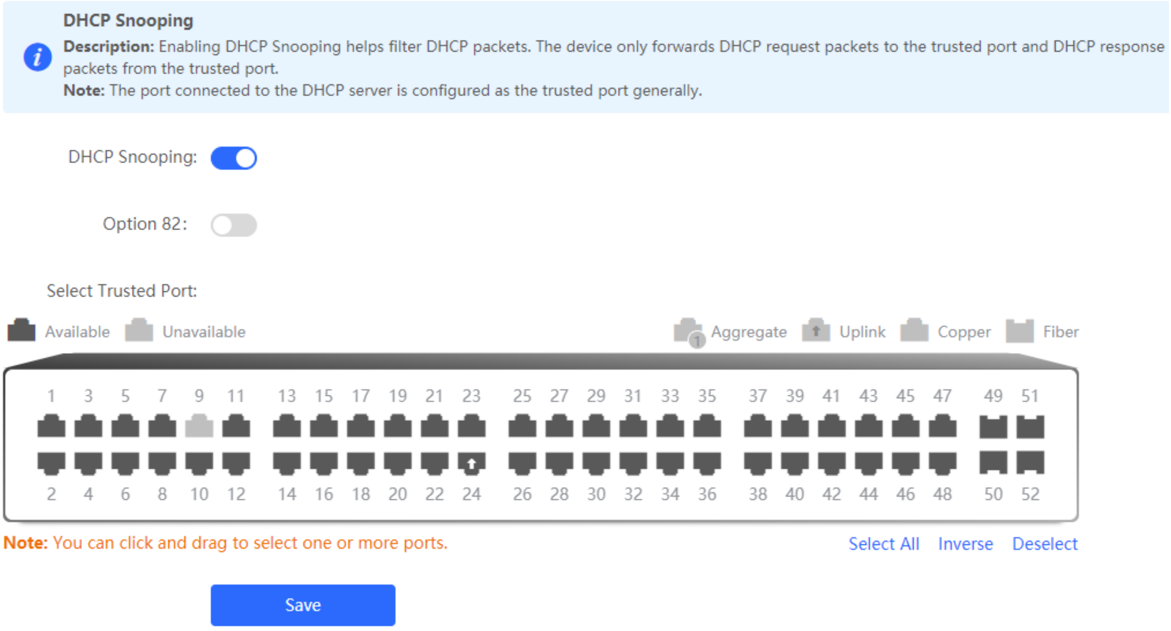
Choose **Local Device** > **Security** > **DHCP Snooping**.

Turn on the DHCP snooping function, select the port to be set as trusted ports on the port panel and click **Save**. After DHCP Snooping is enabled, request packets from DHCP clients are forwarded only to trusted ports; for response packets from DHCP servers, only those from trusted ports are forwarded.

Note

Generally, the uplink port connected to the DHCP server is configured as a trusted port.

Option 82 is used to enhance the DHCP server security and optimize the IP address assignment policy. Option 82 information will be carried in the DHCP request packet when Option 82 is turned on.



DHCP Snooping

Description: Enabling DHCP Snooping helps filter DHCP packets. The device only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port.

Note: The port connected to the DHCP server is configured as the trusted port generally.

DHCP Snooping: ●

Option 82: ○

Select Trusted Port:

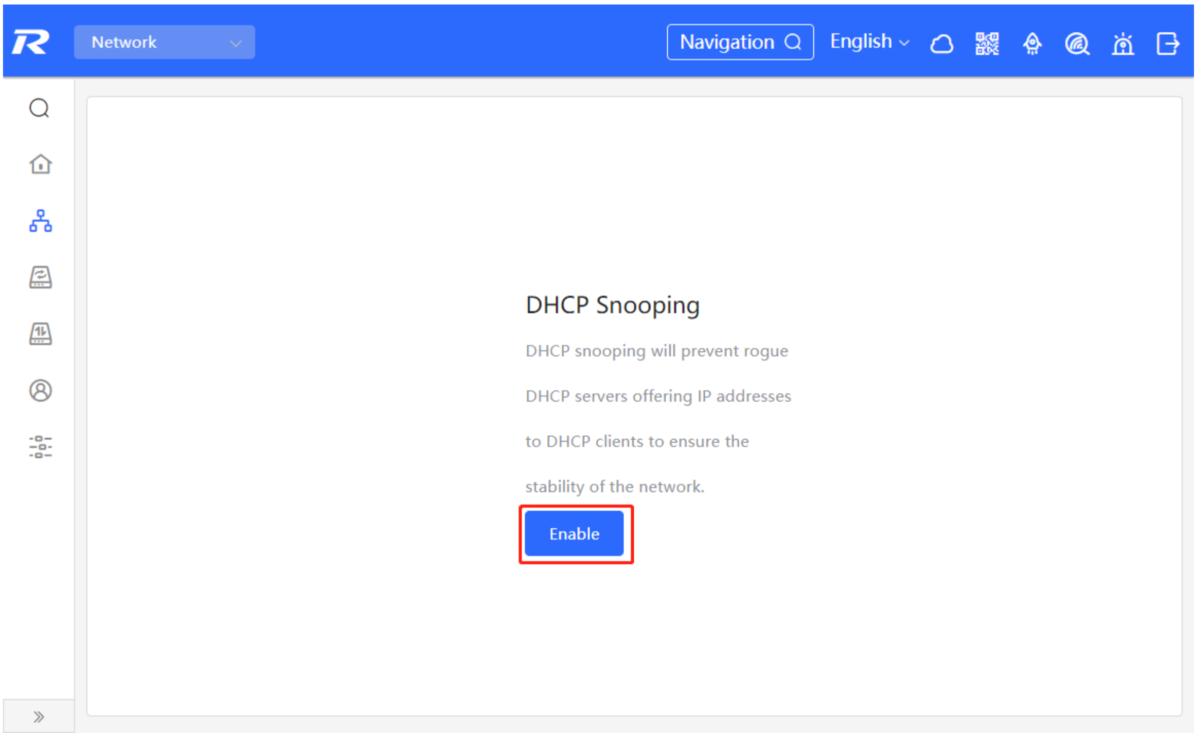
Note: You can click and drag to select one or more ports.

15.1.3 Batch Configuring Network Switches

Choose **Network** > **DHCP Snooping**.

Enabling DHCP Snooping on network switches can ensure that users can only obtain network configurationparameters from the DHCP server within the control range, and avoid the occurrence of “the Internet terminal in the original network obtains the IP address assigned by the privately accessed router”, to guarantee the stability of the network.

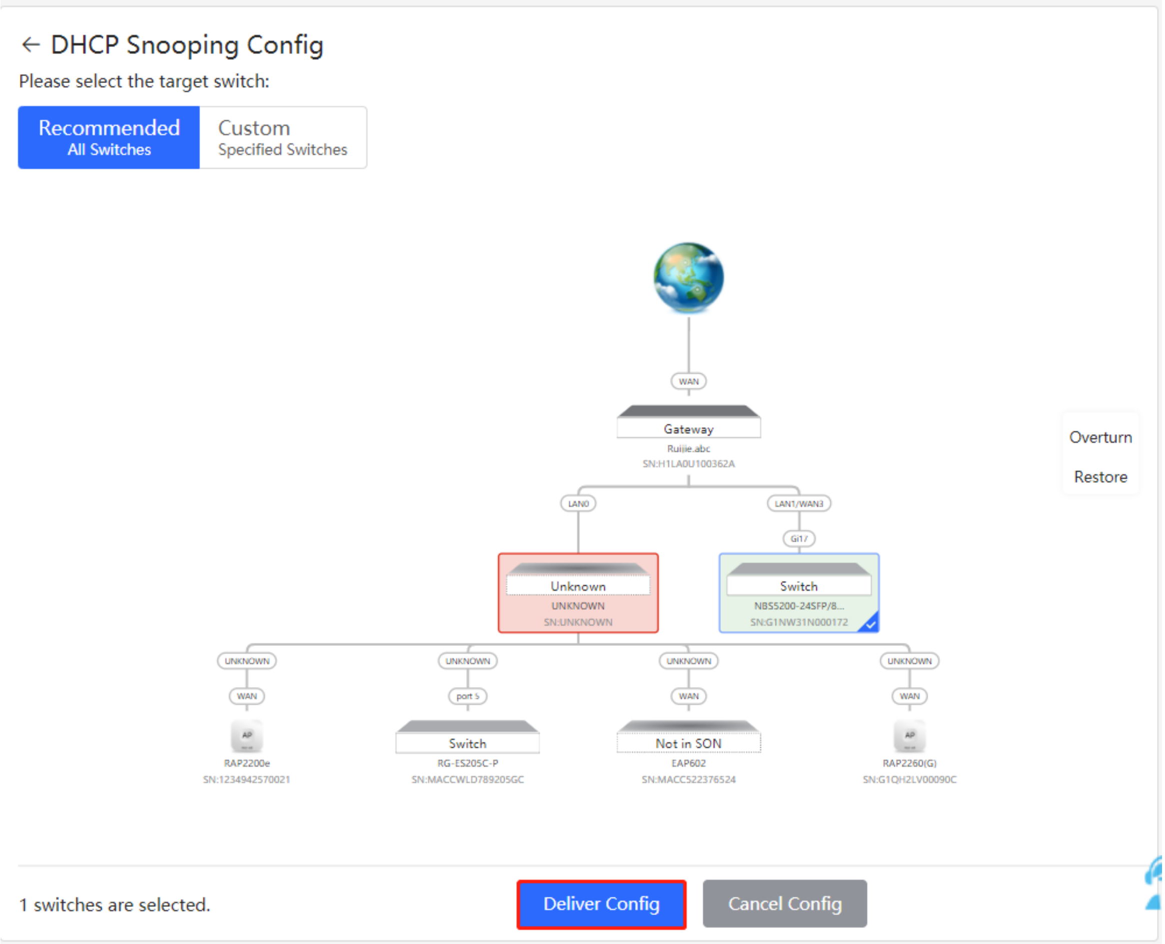
(1) Click **Enable** to access the **DHCP Snooping Config** page.



DHCP Snooping

DHCP snooping will prevent rogue DHCP servers offering IP addresses to DHCP clients to ensure the stability of the network.

(2) In the networking topology, you can select the access switches on which you want to enable DHCP Snooping in either recommended or custom mode. If you select the recommended mode, all switches in the network are selected automatically. If you select the custom mode, you can manually select the desired switches. Click **Deliver Config**. DHCP Snooping is enabled on the selected switches.

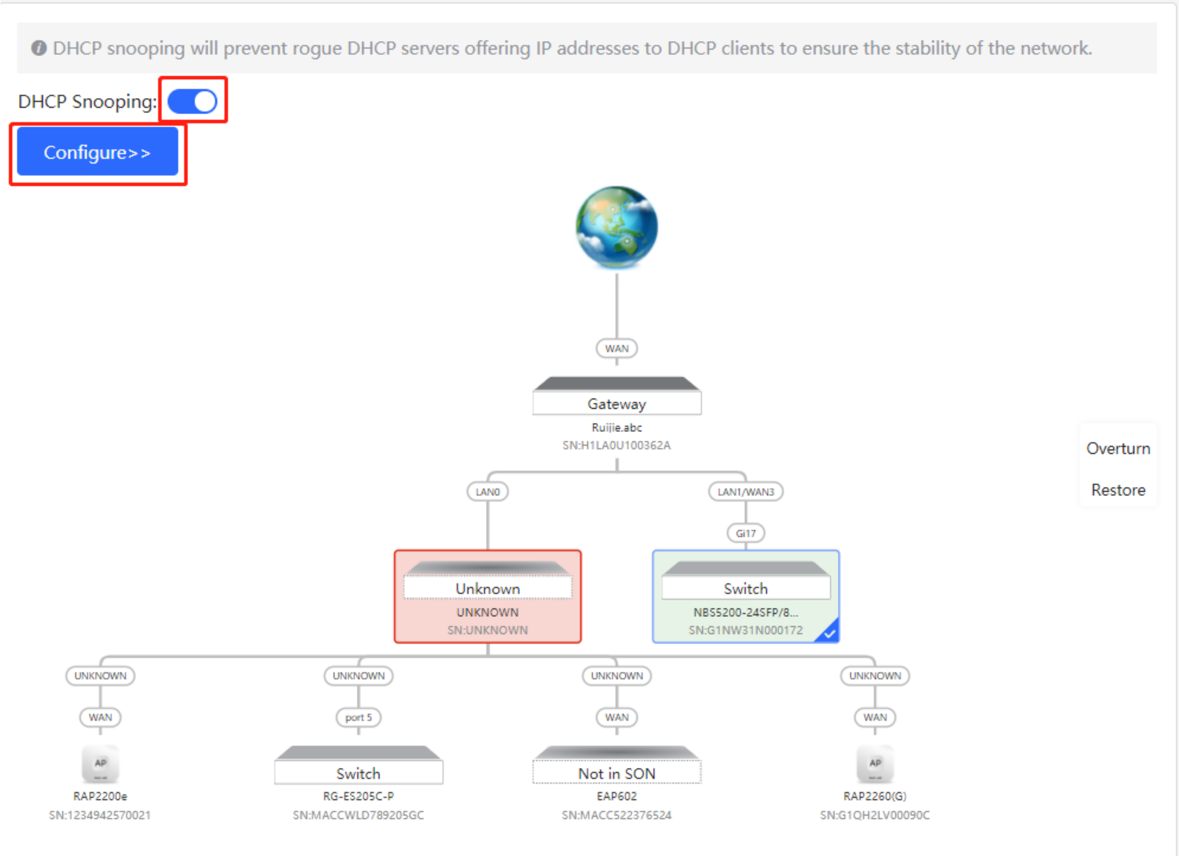


← DHCP Snooping Config

Please select the target switch:

1 switches are selected.

(3) After the configuration is delivered, if you need to modify the effective range of the anti-private connection function, click **Configure** to reselect the switch that enables the anti-private connection in the topology.After the configuration is delivered, if you want to modify the effective range of the DHCP Snooping function, click **Configure** to select desired switches in the topology again. Turn off **DHCP Snooping** to disable DHCP Snooping on all switches with one click.



DHCP snooping will prevent rogue DHCP servers offering IP addresses to DHCP clients to ensure the stability of the network.

DHCP Snooping: ●

15.2 Storm Control

15.2.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This is called LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

Users can perform storm control separately for the broadcast, multicast, and unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

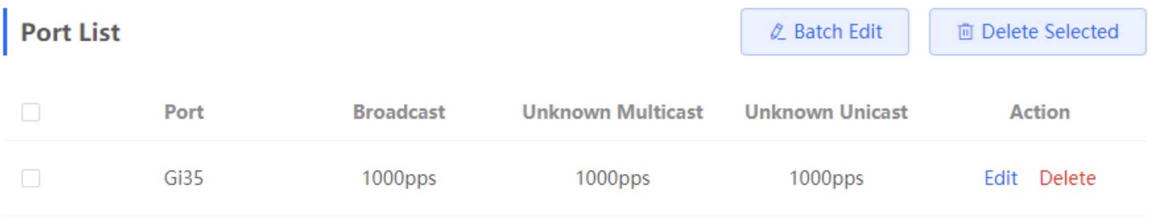
15.2.2 Procedure

Choose **Local Device** > **Security** > **Storm Control**.

Click **Batch Edit**. In the displayed dialog box, select configuration types and ports, enter the rate limits of broadcast, unknown multicast, and unknown unicast, and click **OK**. To modify or delete the rate limit rules after completing the configuration, you can click **Edit** or **Delete** in the **Action** column.

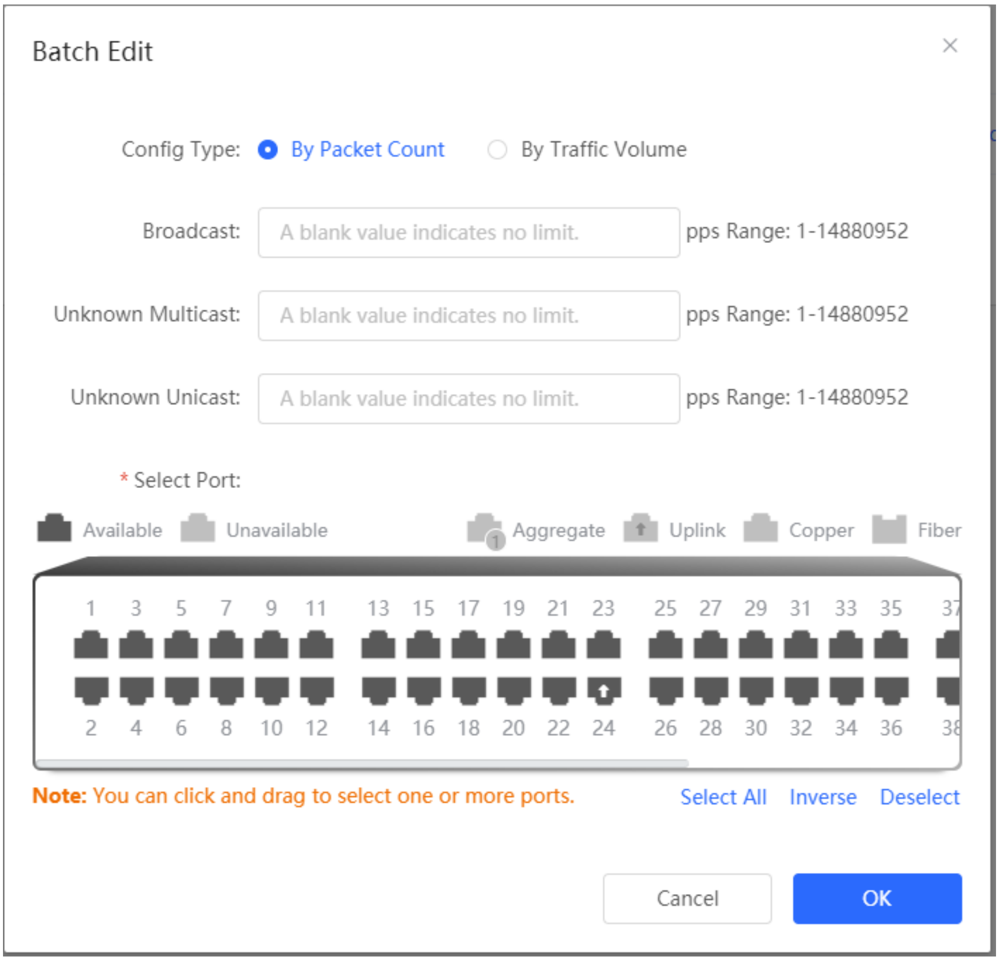
There are two configuration types:

- Storm control based on packets per second: If the rate of data flows received over a device port exceeds the configured packets-per-second threshold, excess data flows are discarded until the rate falls within the threshold.
- Storm control based on kilobytes per second: If the rate of data flows received over a device port exceeds the configured kilobytes-per-second threshold, excess data flows are discarded until the rate falls within the threshold.



Port List

□	Port	Broadcast	Unknown Multicast	Unknown Unicast	Action
□	Gi35	1000pps	1000pps	1000pps	Edit Delete



Batch Edit

Config Type: ● By Packet Count ○ By Traffic Volume

Broadcast: A blank value indicates no limit. pps Range: 1-14880952

Unknown Multicast: A blank value indicates no limit. pps Range: 1-14880952

Unknown Unicast: A blank value indicates no limit. pps Range: 1-14880952

* Select Port:

Note: You can click and drag to select one or more ports.

15.3 ACL

15.3.1 Overview

An access control list (ACL) is commonly referred to as packet filter in some documents. An ACL defines a series of permit or deny rules and applies these rules to device interfaces to control packets sent to and from the interfaces, so as to enhance security of the network device.

You can add ACLs based on MAC addresses or IP addresses and bind ACLs to ports.

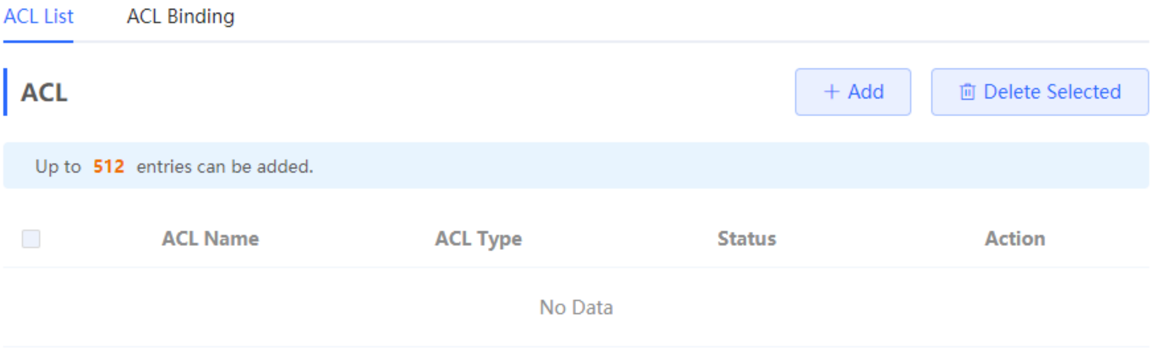
15.3.2 Creating ACL Rules

Choose **Local Device** > **Security** > **ACL** > **ACL List**.

(1) Click **Add** to set the ACL control type, enter an ACL name, and click **OK**.

Based on MAC address: To control the L2 packets entering/leaving the port, and deny or permit specific L2 packets destined to a network.

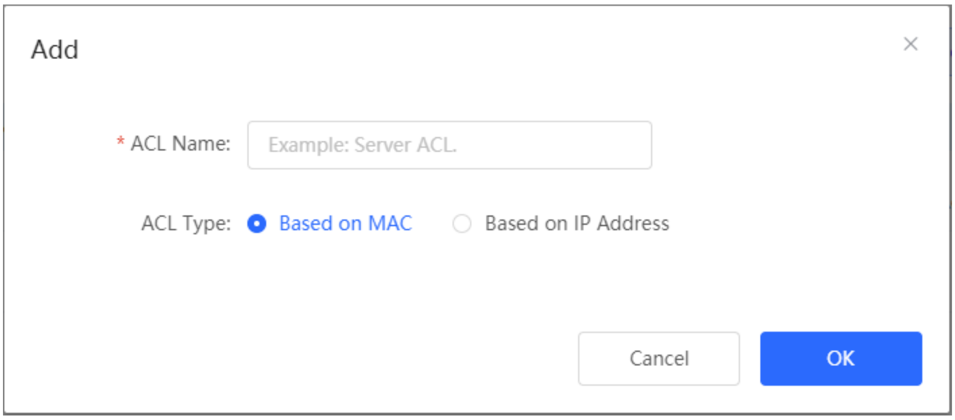
Based on IP address: To control the Ipv4 packets entering/leaving a port, and deny or permit specific Ipv4 packets destined to a network.



Up to 512 entries can be added.

□	ACL Name	ACL Type	Status	Action

No Data

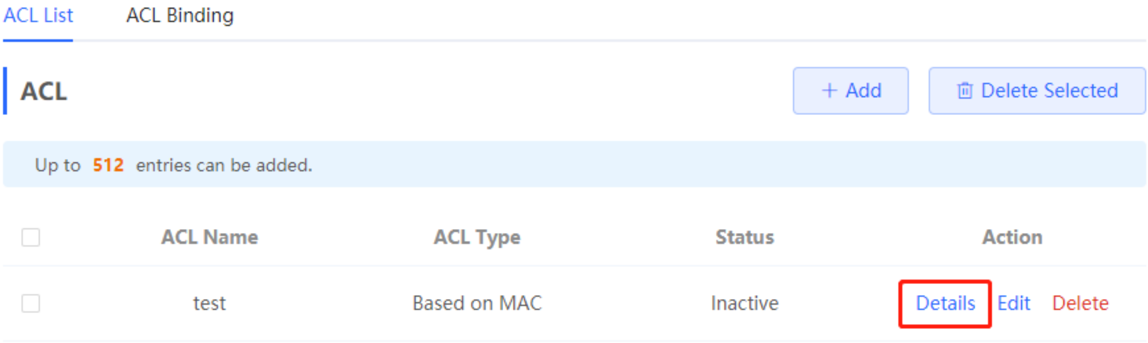


* ACL Name: Example: Server ACL.

ACL Type: ● Based on MAC ○ Based on IP Address

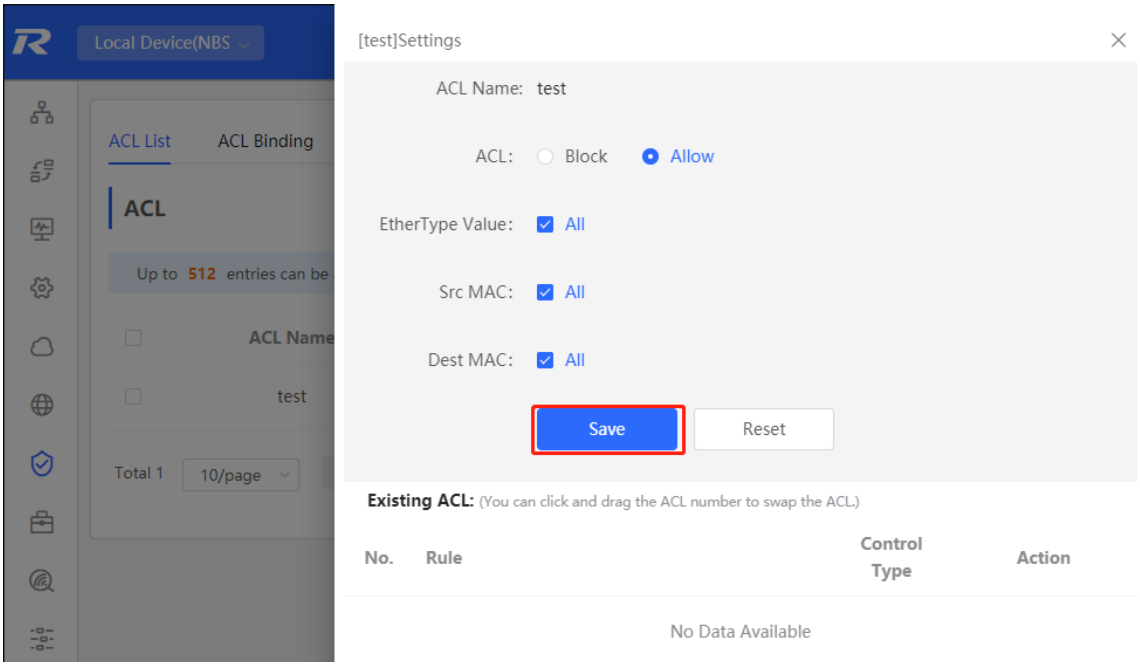
(2) Click **Details** in the **Action** column of the ACL entry, set the filtering rules in the pop-up sidebar, and click **Save** to add rules for the ACL. Multiple rules can be added.

The rules include two actions of **Allow** or **Block**, and the matching rules of packets. The sequence of a Rule in an ACL determines the matching priority of the Rule in the ACL. When processing packets, the network device matches packets with ACEs based on the Rule sequence numbers. Click **Move** in the rule list to adjust the matching order.



Up to 512 entries can be added.

□	ACL Name	ACL Type	Status	Action
□	test	Based on MAC	Inactive	Details Edit Delete



[test]Settings

ACL Name: test

ACL: ○ Block ● Allow

EtherType Value: ☑ All

Src MAC: ☑ All

Dest MAC: ☑ All

Save Reset

Existing ACL: (You can click and drag the ACL number to swap the ACL.)

No.	Rule	Control Type	Action

No Data Available

Table 7-1 Description of ACL Rule Configuration Parameters

Parameter	Description
ACL	Configuring ACL Rules Action Block: If packets match this rule, the packets are denied. Allow: If packets match this rule, the packets are permitted.
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check All to match all IP protocols.
Src IP Address	Match the source IP address of the packet. Check All to match all source IP addresses.
Dest IP Address	Match the destination IP address of the packet. Check All to match all destination IP addresses
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to match all protocol type numbers.
Src Mac	Match the MAC address of the source host. Check All to match all source MAC addresses
Dest MAC	Match the MAC address of the destination host. Check All to match all destination MAC addresses

Note

- ACLs cannot have the same name. Only the name of a created ACL can be edited.
- An ACL applied by a port cannot be edited or deleted. To edit, unbind the ACL from the port first.
- There is one default ACL rule that denies all packets hidden at the end of an ACL.

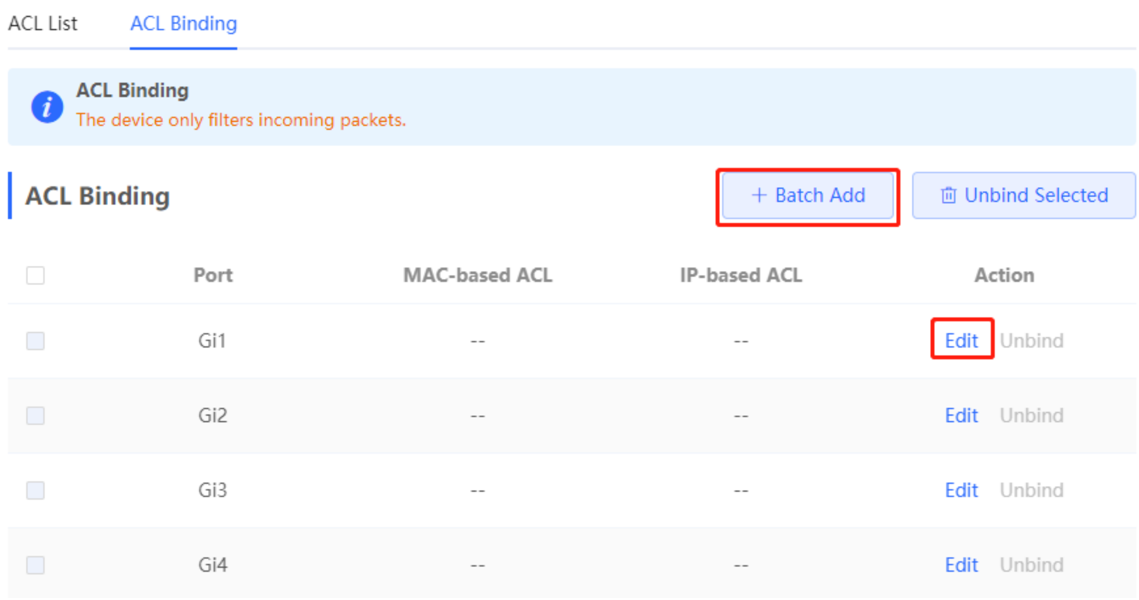
15.3.3 Applying ACL Rules

Choose **Local Device** > **Security** > **ACL** > **ACL List**.

Click **Batch Add** or **Edit** in the **Action** column, select the desired MAC ACL and IP ACL for ports, and click **OK**.

Note

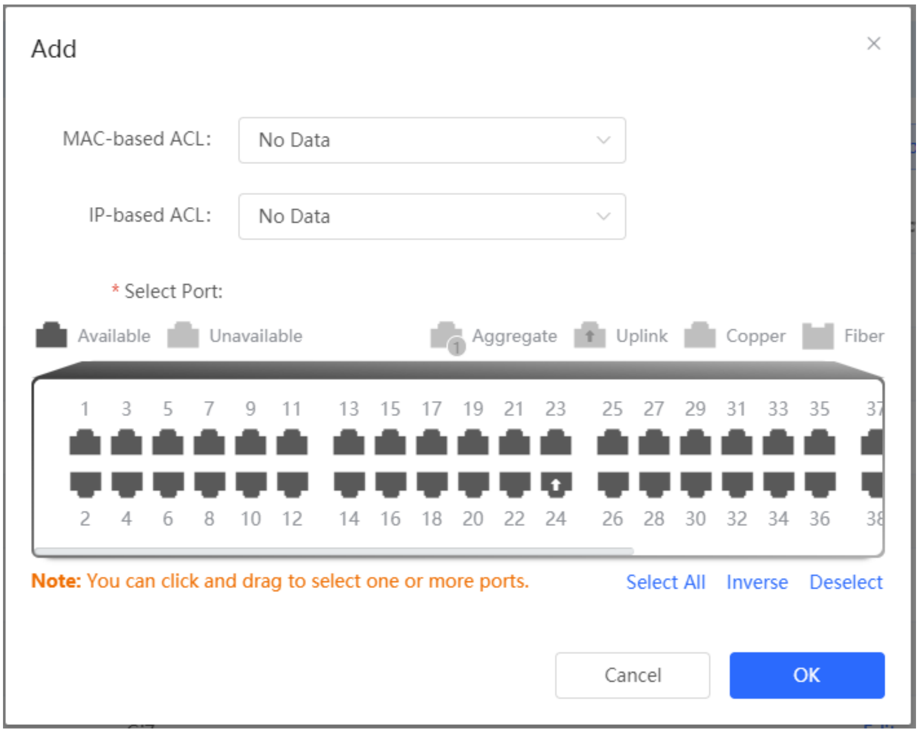
Currently, ACLs can be applied only in the inbound direction of ports, that is, to filter incoming packets.



ACL Binding
The device only filters incoming packets.

ACL Binding

□	Port	MAC-based ACL	IP-based ACL	Action
□	Gi1	--	--	Edit Unbind
□	Gi2	--	--	Edit Unbind
□	Gi3	--	--	Edit Unbind
□	Gi4	--	--	Edit Unbind



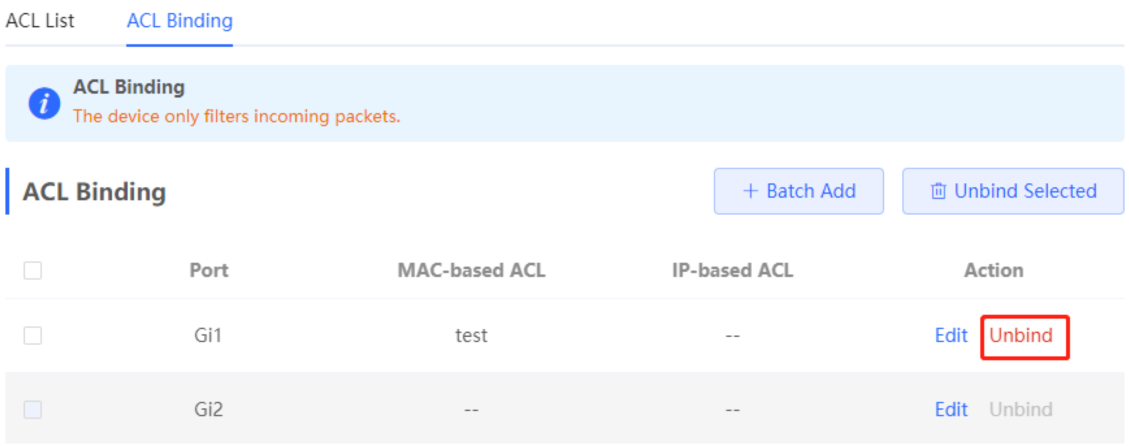
MAC-based ACL: No Data

IP-based ACL: No Data

* Select Port:

Note: You can click and drag to select one or more ports.

After an ACL is applied to a port, you can click **Unbind** in the **Action** column, or check the port entry and click **Delete Selected** to unbind the ACL from the port.



ACL Binding

The device only filters incoming packets.

ACL Binding

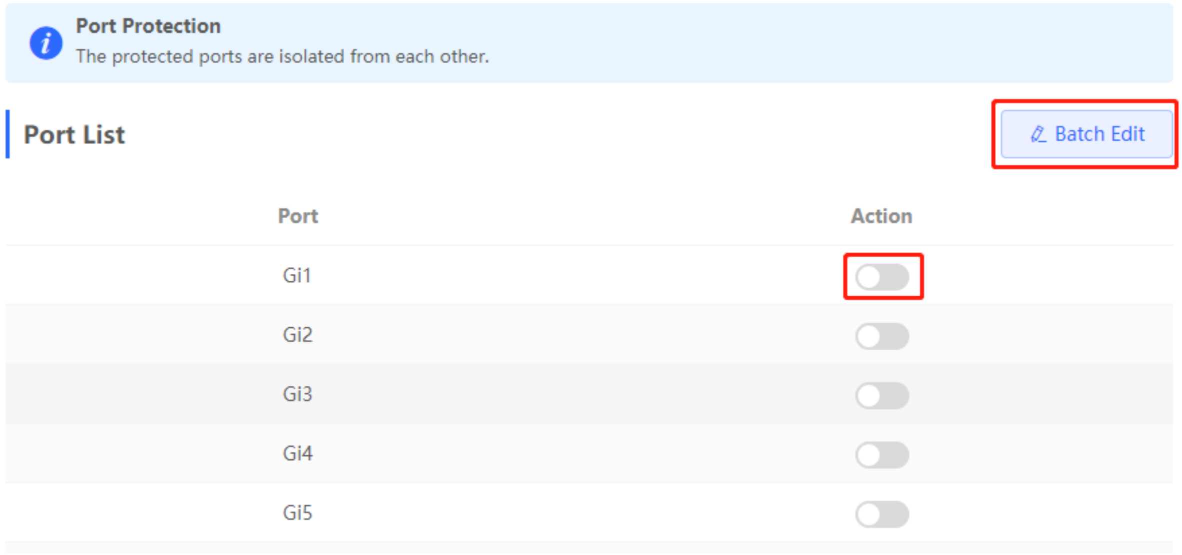
□	Port	MAC-based ACL	IP-based ACL	Action
□	Gi1	test	--	Edit Unbind
□	Gi2	--	--	Edit Unbind

15.4 Port Protection

Choose **Local Device** > **Security** > **Port Protection**.

In some scenarios, it is required that communication be disabled between some ports on the device. For this purpose, you can configure some ports as protected ports. Ports that enable port protection (protected ports) cannot communicate with each other, users on different ports are L2-isolated. The protected ports can communicate with non-protected ports.

Port protection is disabled by default, which can be enabled by clicking to batch enable port protection for multiple ports, you can click **Batch Edit** to enable port protection**,** select desired port and click **OK.**



Port Protection

The protected ports are isolated from each other.

Port List

Port	Action
Gi1	○
Gi2	○
Gi3	○
Gi4	○
Gi5	○

15.5 IP-MAC Binding

15.5.1 Overview

After IP-MAC binding is configured on a port, to improve security, the device checks whether the source IP addresses and source MAC addresses of IP packets are those configured for the device, filters out IP packets not matching the binding, and strictly control the validity of input sources.

15.5.2 Procedure

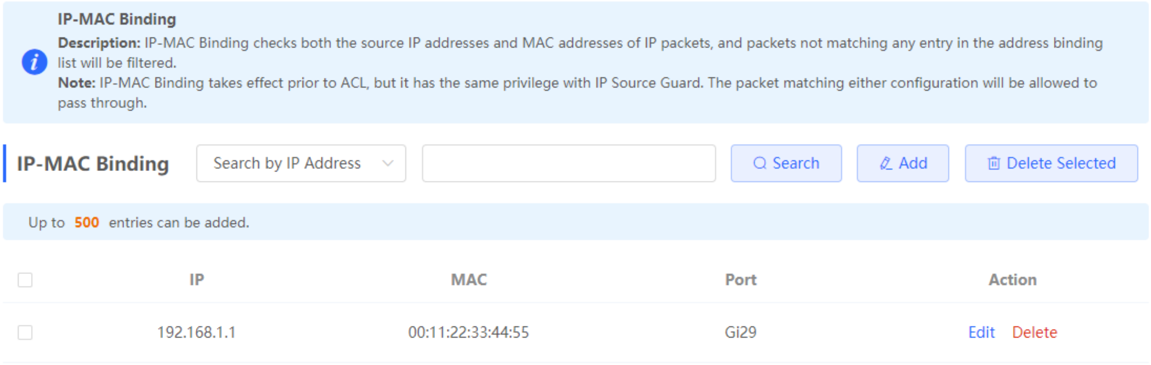
Choose **Local Device** > **Security** > **IP-MAC Binding**.

1. Adding an IP-MAC Binding Entry

Click **Add**, select the desired port, enter the IP address and MAC address to be bound, and click **OK**. At least one of the IP address and MAC address needs to be entered. To modify the binding, you can click **Edit** in the **Action** column.

⚠ **Caution**

IP-MAC Binding take effects prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.



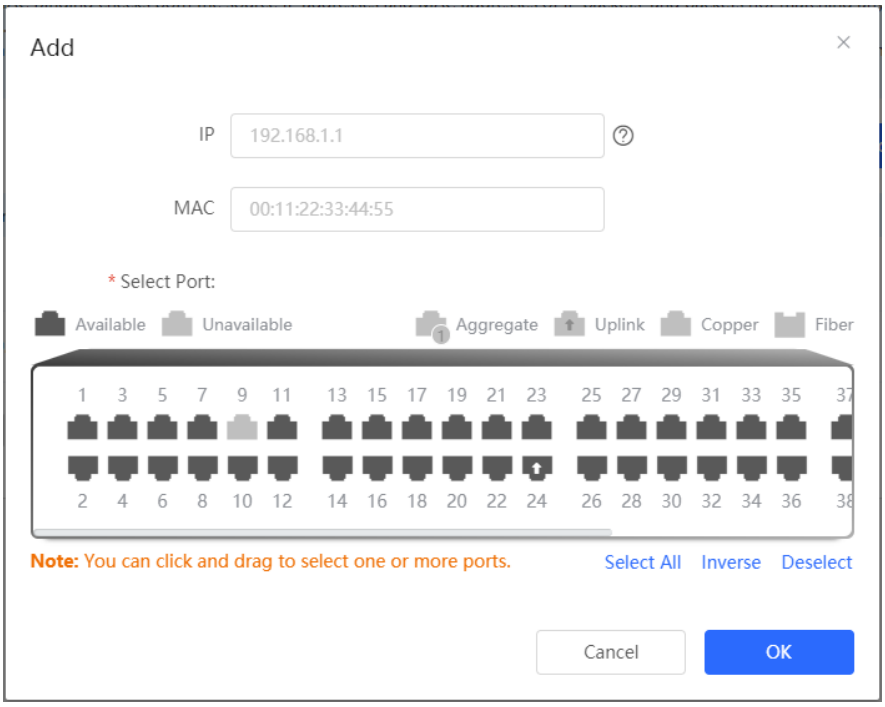
IP-MAC Binding

Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding list will be filtered.

Note: IP-MAC Binding takes effect prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.

Up to 500 entries can be added.

□	IP	MAC	Port	Action
□	192.168.1.1	00:11:22:33:44:55	Gi29	Edit Delete



Add

IP: 192.168.1.1

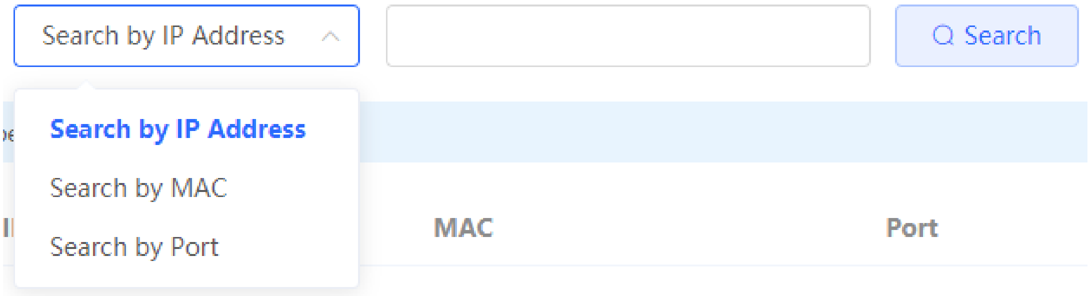
MAC: 00:11:22:33:44:55

* Select Port:

Note: You can click and drag to select one or more ports.

2. Searching Binding Entries

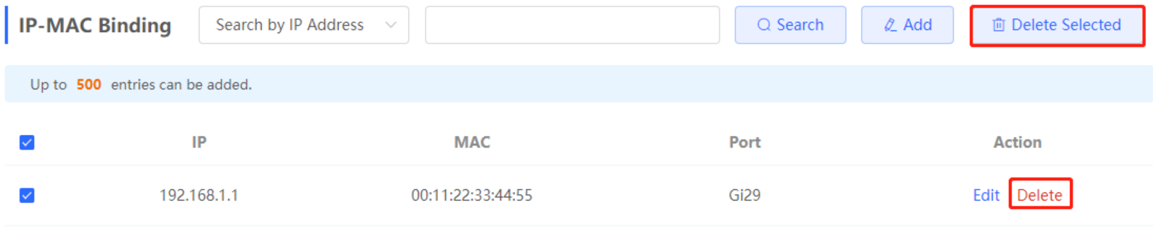
The search box in the upper-right corner supports finding binding entries based on IP addresses, MAC addresses or ports. Select the search type, enter the search string, and click **Search**. Entries that meet the search criteria are displayed in the list.



3. **Deleting an IP-MAC Binding Entry**

Batch Configure: In **IP-MAC Binding List**, select an entry to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.

Delete one binding entry: click **Delete** in the last **Action** column of the entry in the list. In the displayed dialog box, click **OK**.



Up to 500 entries can be added.

☑	IP	MAC	Port	Action
☑	192.168.1.1	00:11:22:33:44:55	Gi29	Edit Delete

15.6 IP Source Guard

15.6.1 Overview

After the IP Source Guard function is enabled, the device checks IP packets from DHCP non-trusted ports. You can configure the device to check only the IP field or IP+MAC field to filter out IP packets not matching the binding list. It can prevent users from setting private IP addresses and forging IP packets.

⚠ **Caution**

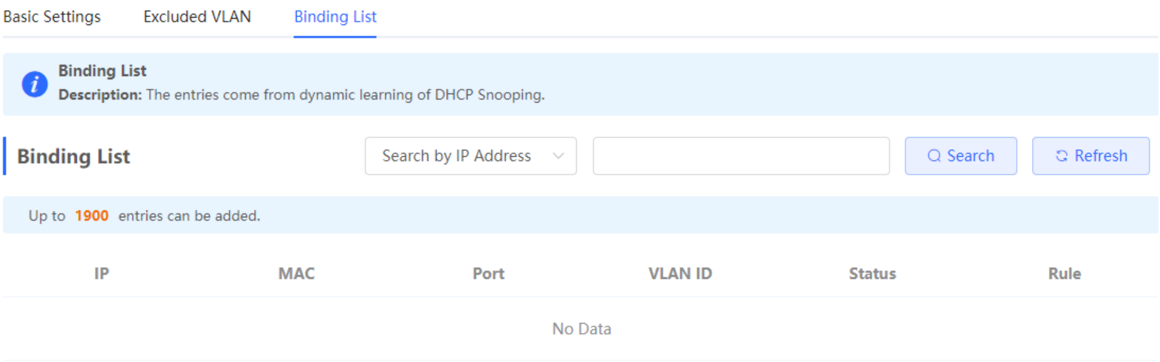
IP Source Gusrd should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see 7.1 for details.

15.6.2 Viewing Binding List

Choose **Local Device** > **Security** > **IP Source Guard** > **Binding List**.

The binding list is the basis for IP Source Guard. Currently, data in **Binding List** is sourced from dynamic learning results of DHCP snooping binding database. When IP Source Guard is enabled, data of the DHCP Snooping binding database is synchronized to the binding list of IP Source Guard. In this case, IP packets are filtered strictly through IP Source Guard on devices with DHCP Snooping enabled.

Click **Refresh** to obtain the latest data in **Binding List**.



Binding List

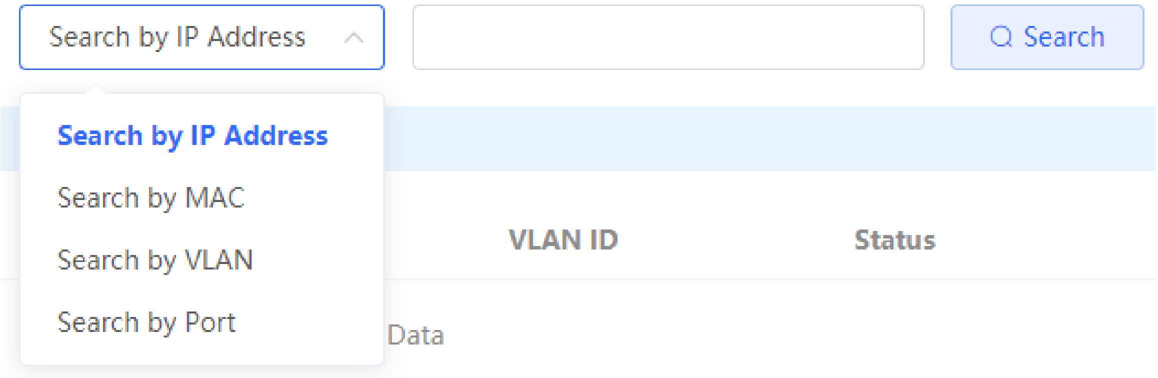
Description: The entries come from dynamic learning of DHCP Snooping.

Binding List

Up to 1900 entries can be added.

IP	MAC	Port	VLAN ID	Status	Rule
No Data					

The search box in the upper-right corner supports finding the specified entry in **Binding List** based on IP addresses, MAC addresses, VLANs or ports. Click the drop-down list box to select the search type, enter the search string, and click **Search**.



15.6.3 Enabling Port IP Source Guard

Choose **Local Device** > **Security** > **IP Source Guard** > **Basic Settings**.

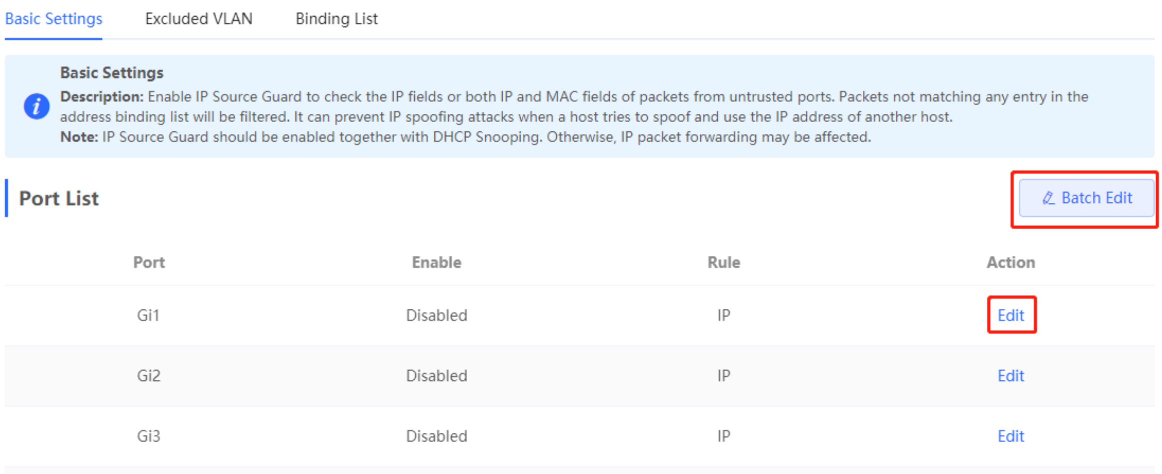
In Port List, click **Edit** in the **Action** column. Select **Enabled** and select the match rule, and click **OK**.

There are two match rules:

- IP address: The source IP addresses of all IP packets passing through the port are checked. Packets are allowed to pass through the port only when the source IP addresses of these packets match those in the binding list.
- IP address+ MAC address: The source IP addresses and MAC addresses of IP packets passing through the port are checked. Packets are allowed to pass through the port only when both the L2 source MAC addresses and L3 source IP addresses of these packets match an entry in the binding list.

Caution

- IP Source Guard is not supported to be enabled on a DHCP Snooping trusted port.
- Only on an L2 interface is IP Source Guard supported to be enabled.



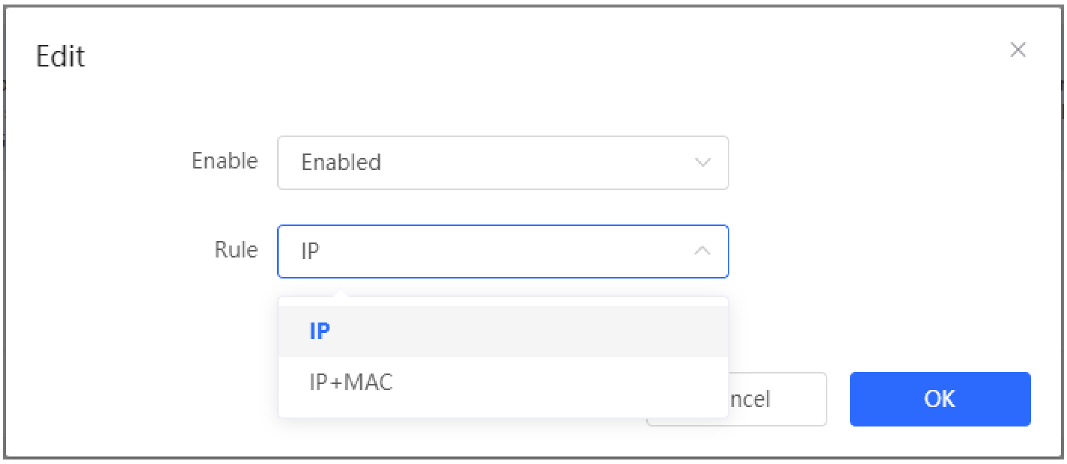
Basic Settings

Description: Enable IP Source Guard to check the IP fields or both IP and MAC fields of packets from untrusted ports. Packets not matching any entry in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

Note: IP Source Guard should be enabled together with DHCP Snooping. Otherwise, IP packet forwarding may be affected.

Port List

Port	Enable	Rule	Action
Gi1	Disabled	IP	Edit
Gi2	Disabled	IP	Edit
Gi3	Disabled	IP	Edit



Edit

Enable: Enabled

Rule: IP

15.6.4 Configuring Exceptional VLAN Addresses

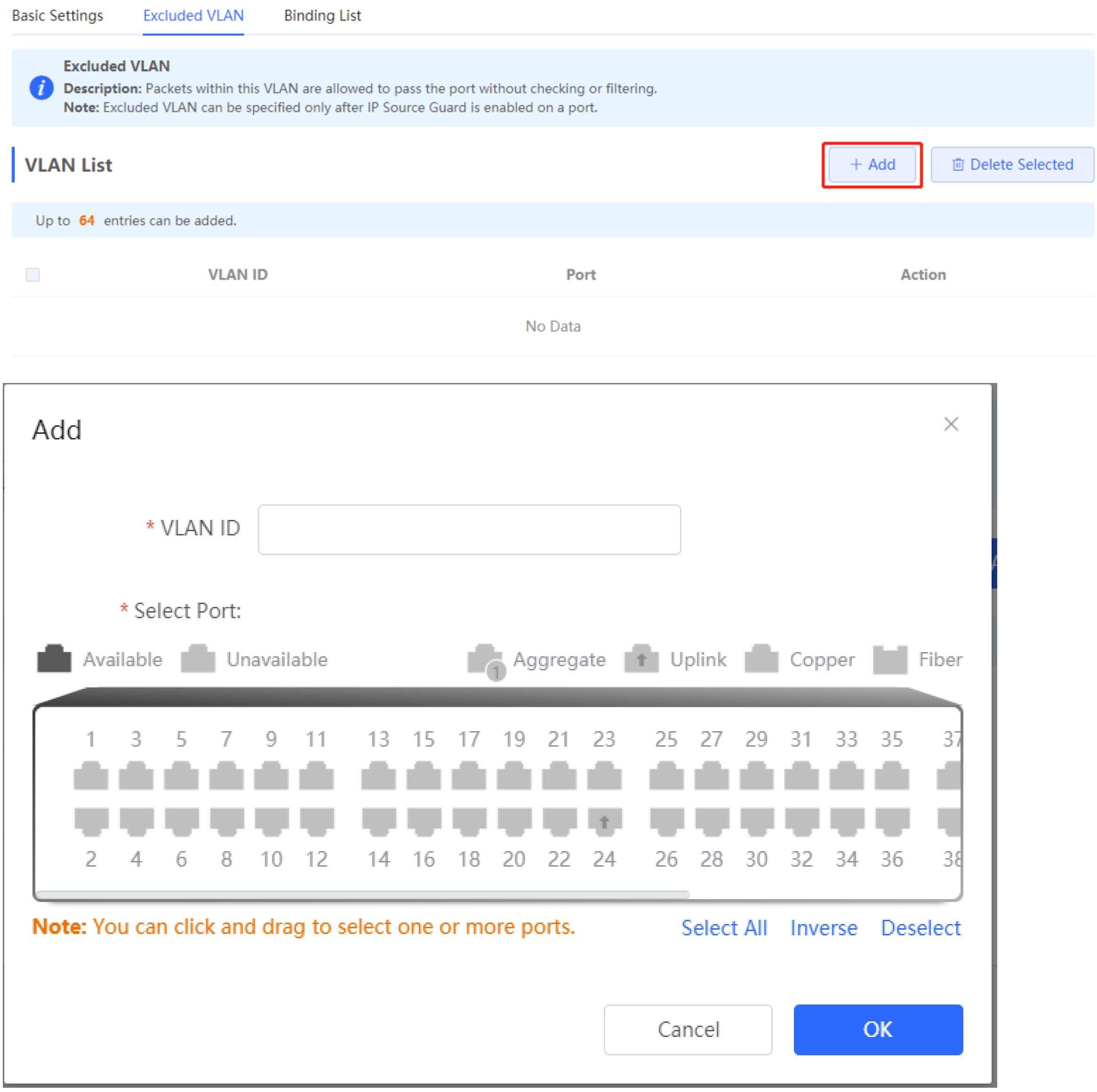
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard.

Click **Edit**, enter the Excluded VLAN ID and the desired port, and click **OK**.

Caution

Excluded VLANs can be specified on a port only after IP Source Guard is enabled on the port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on the port.



Basic Settings | Excluded VLAN | Binding List

Excluded VLAN

Description: Packets within this VLAN are allowed to pass the port without checking or filtering.

Note: Excluded VLAN can be specified only after IP Source Guard is enabled on a port.

VLAN List

+ Add | Delete Selected

Up to 64 entries can be added.

□	VLAN ID	Port	Action
		No Data	

Add

* VLAN ID

* Select Port:

Note: You can click and drag to select one or more ports.

15.7 Anti-ARP Spoofing

15.7.1 Overview

Gateway-targeted ARP spoofing prevention is used to check whether the source IP address of an ARP packet through an access port is set to the gateway IP address. If yes, the packet will be discarded to prevent hosts from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the uplink devices can send ARP packets, and the ARP response packets sent from other clients which pass for the gateway are filtered out.

15.7.2 Procedure

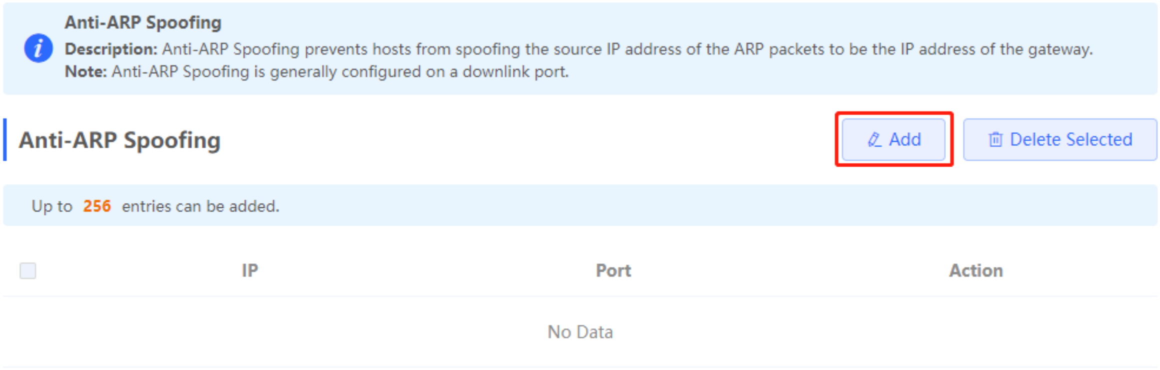
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

1. **Enabling Anti-ARP Spoofing**

Click **Add**, select the desired port and enter the gateway IP, click **OK**.

Note

Generally, the anti-ARP spoofing function is enabled on the downlink ports of the device.



Anti-ARP Spoofing

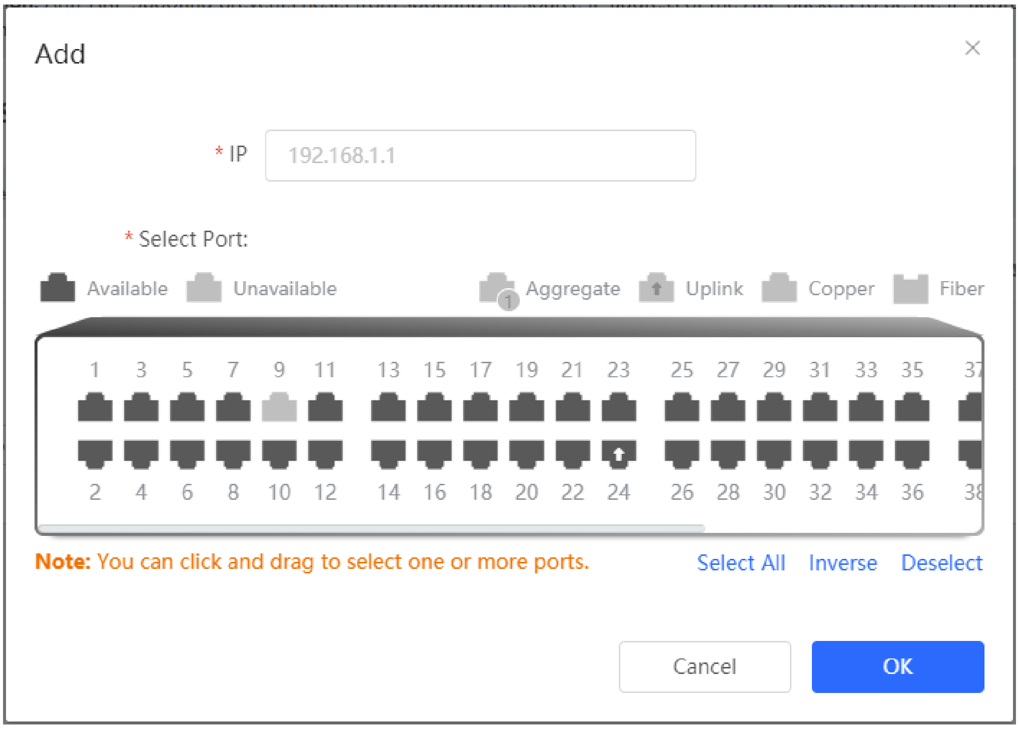
Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.

Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

Up to 256 entries can be added.

□	IP	Port	Action
No Data			



Add

* IP: 192.168.1.1

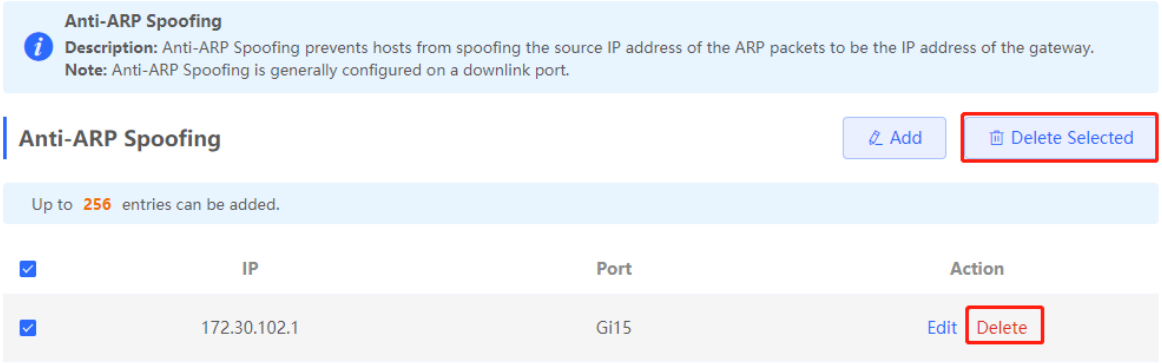
* Select Port:

Note: You can click and drag to select one or more ports.

2. Disabling Anti-ARP Spoofing

Batch disable: Select an entry to be deleted in the list and click **Delete Selected**.

Disable one port: click **Delete** in the last **Action** column of the corresponding entry.



Anti-ARP Spoofing

Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.

Note: Anti-ARP Spoofing is generally configured on a downlink port.

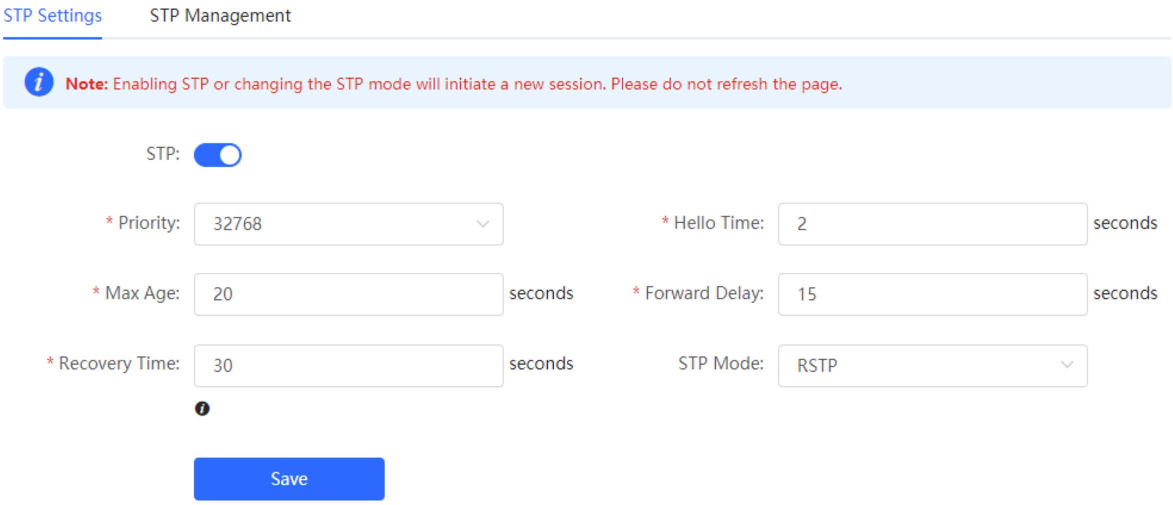
Up to 256 entries can be added.

☑	IP	Port	Action
☑	172.30.102.1	Gi15	Edit Delete

16 NBS Series Advanced Configuration

16.1 STP

STP (Spanning Tree Protocol) is an L2 management protocol that eliminates L2 loops by selectively blocking redundant links in the network. It also provides the link backup function.



Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP: ●

* Priority: 32768

* Hello Time: 2 seconds

* Max Age: 20 seconds

* Forward Delay: 15 seconds

* Recovery Time: 30 seconds

STP Mode: RSTP

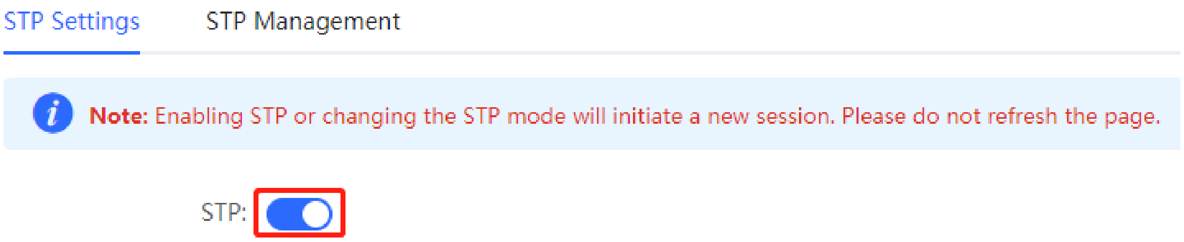
16.1.1 STP Global Settings

Choose **Local Device** > **Advanced** > **STP** > **STP**.

(1) Click to to enable the STP function, and click OK in the displayed box. The STP function is disabled by default.

Notice **Caution**

Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.



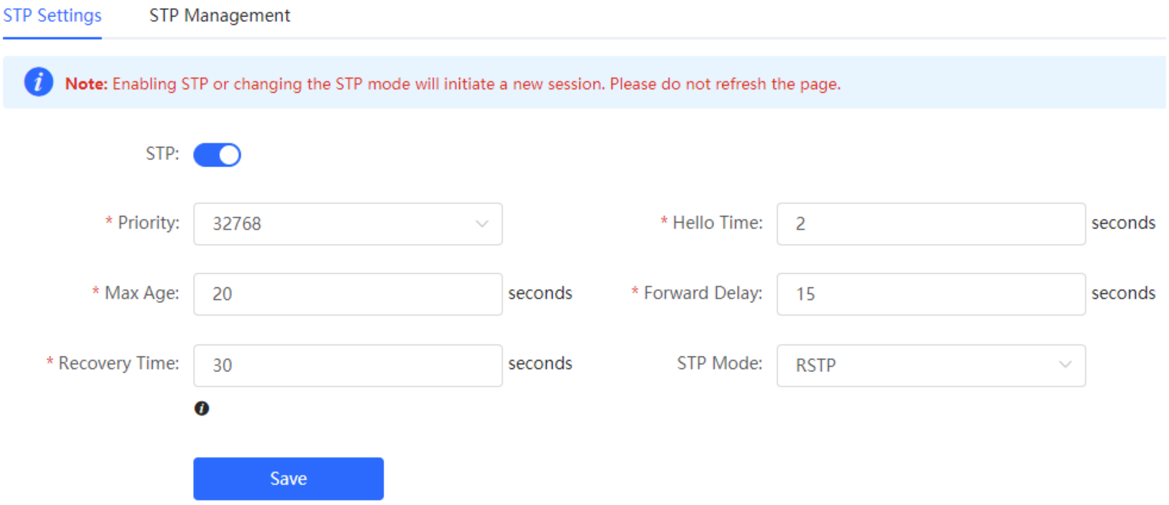
STP Settings

STP Management

Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP:

(2) Configure the STP global parameters, and click **Save**.



STP Settings

STP Management

Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP:

* Priority: 32768

* Hello Time: 2 seconds

* Max Age: 20 seconds

* Forward Delay: 15 seconds

* Recovery Time: 30 seconds

STP Mode: RSTP

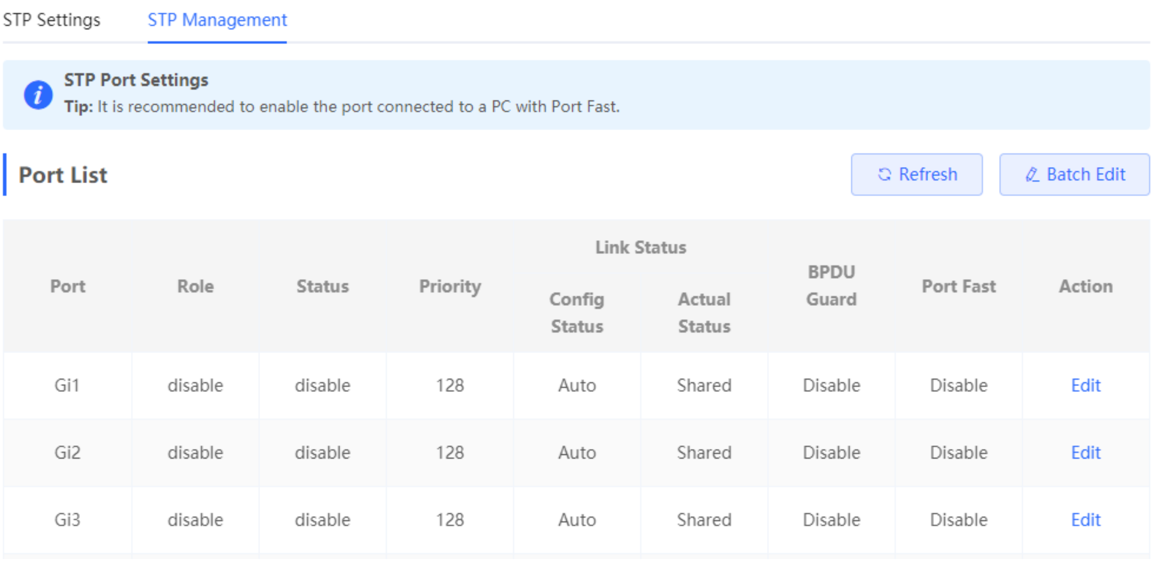
Table 8-1 Description of STP Global Configuration Parameters

Parameter	Description	Default Value
STP	Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled.	Disable
Priority	Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher priority.	32768
Max Age	The maximum expiration time of BPDUs The packets expiring will be discarded. If a non-root bridge fails to receive a BPDU from the root bridge before the aging time expires, the root bridge or the link to the root bridge is deemed as faulty	20 seconds
Recovery Time	Network recovery time when redundant links occur on the network.	30 seconds
Hello Time	Interval for sending two adjacent BPDUs	2 seconds
Forward Delay	The interval at which the port status changes, that is, the interval for the port to change from Listening to Learning, or from Learning to Forwarding.	15 seconds
STP Mode	The versions of Spanning Tree Protocol. Currently the device supports STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol).	RSTP

16.1.2 Applying STP to a Port

Choose **Local Device** > **Advanced** >**STP** > **STP**.

Configure the STP properties for a port Click **Batch Edit** to select ports and configure STP parameters, or click **Edit** in the **Action** column in **Port List** to configure designated ports.

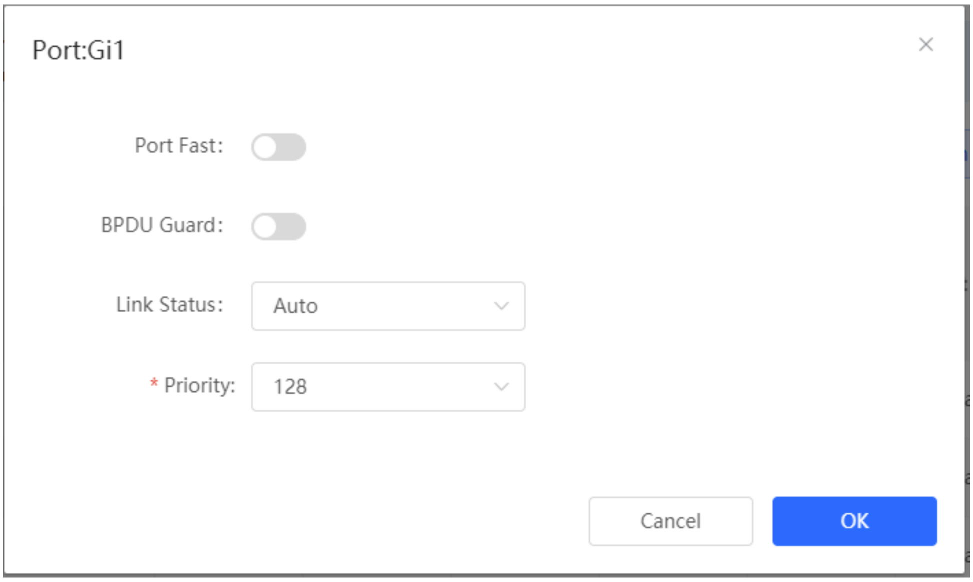


STP Port Settings

Tip: It is recommended to enable the port connected to a PC with Port Fast.

Port List

Port	Role	Status	Priority	Link Status		BPDU Guard	Port Fast	Action
				Config Status	Actual Status			
Gi1	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi3	disable	disable	128	Auto	Shared	Disable	Disable	Edit



Port:Gi1

Port Fast:

BPDU Guard:

Link Status: Auto

* Priority: 128

Table 8-2 Description of STP Configuration Parameters of Ports

Parameter	**Description**	**Default Value**
Role	Root: A port with the shortest path to the root Alternate: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately. Designated (designated ports): A port that connects a root bridge or a upstream bridge to a downstream device. Disable (blocked ports): Ports that have no effect in the spanning tree.	NA
Status	Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. Listening: If a port can become the root port or designated port, the port will enter the listening state. Listening: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. Learning: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. Forwarding: Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs.	NA
Priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Link Status Config Statis	Configure the link type, the options include: Shared, Point-to-Point and Auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared.	Auto
Link Status Actual Status	Actual link type: Shared, Point-to-Point	NA
BPDU Guard	Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port connected to an endpoint, but the port receives BPDUs, the port will be disabled and enters the Error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change.	Disable

Parameter	Description	Default Value
Port Fast	Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDU.s. If a port, on which Port Fast is enabled exits the Port Fast state automatically when it receives BPDUs, the BPDU filter feature is automatically disabled. Generally, the port connected to a PC is enabled with Port Fast.	Disable

Note

- It is recommended to enable Port Fast on the port connected to a PC.
- A port switches to the forwarding state after STP is enabled more than 30 seconds. Therefore transient disconnection may occur and packets cannot be forwarded.

16.2 LLDP

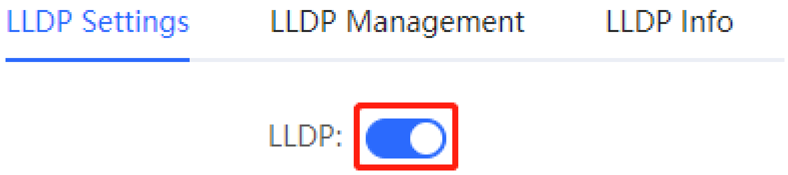
16.2.1 Overview

LLDP (Link Layer Discovery Protocol) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the Eweb management system can learn the topological connection status, for example, ports of the device that are connected to other devices, port rates at both ends of a link, and duplex mode matching status. An administrator can locate and troubleshoot faults quickly based on the preceding information.

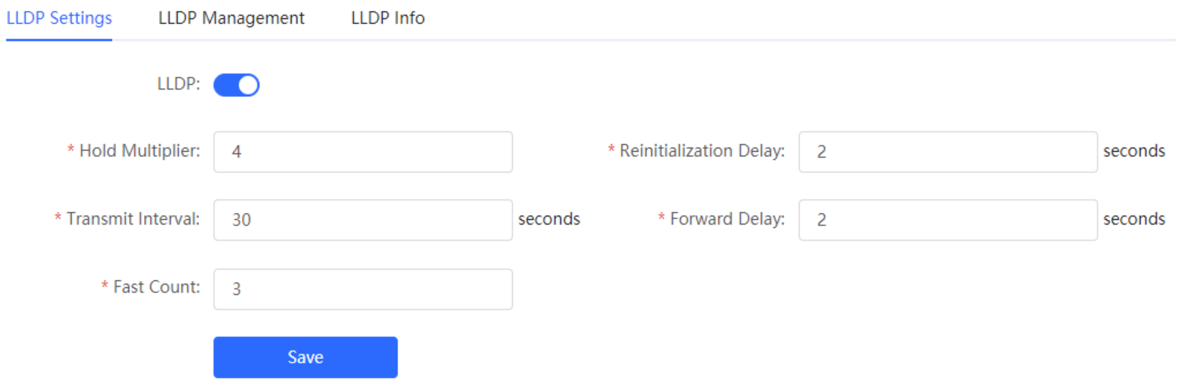
16.2.2 LLDP Global Settings

Choose **Local Device** > **Advanced** >**LLDP** > **LLDP Settings**.

(1) Click to to enable the LLDP function, and click **OK** in the displayed box. The STP function is enabled by default. When the LLDP is enabled, this step can be skipped.



(2) Configure the global LLDP parameters and click **Save**.



LLDP: ●

* Hold Multiplier: 4

* Reinitialization Delay: 2 seconds

* Transmit Interval: 30 seconds

* Forward Delay: 2 seconds

* Fast Count: 3

Table 8-3 Description of LLDP Global Configuration Parameters

Parameter	Description	Default Value
LLDP	Indicates whether the LLDP function is enabled.	Enable
Hold Multiplier	TTL multiplier of LLDP In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor. The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier × Packet transmission interval + 1. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	4
Transmit Interval	Transmission interval of LLDP packets, in seconds The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier × Packet transmission interval + 1. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	30 seconds
Fast Count	Number of packets that are transmitted rapidly When a new neighbor is discovered, or the LLDP working mode is changed, the device will start the fast transmission mechanism in order to let the neighboring devices learn the information of the device as soon as possible. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval. You can configure the number of LLDP packets that can be transmitted rapidly for the fast transmission mechanism.	3
Reinitialization Delay	Port initialization delay, in seconds You can configure an initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.	2 seconds

Parameter	Description	Default Value
Forward Delay	Delay for sending LLDP packets, in seconds. When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information. If the delay is set to a very small value, frequent change of the 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. Set an appropriate delay according to actual conditions.	2 seconds

16.2.3 Applying LLDP to a Port

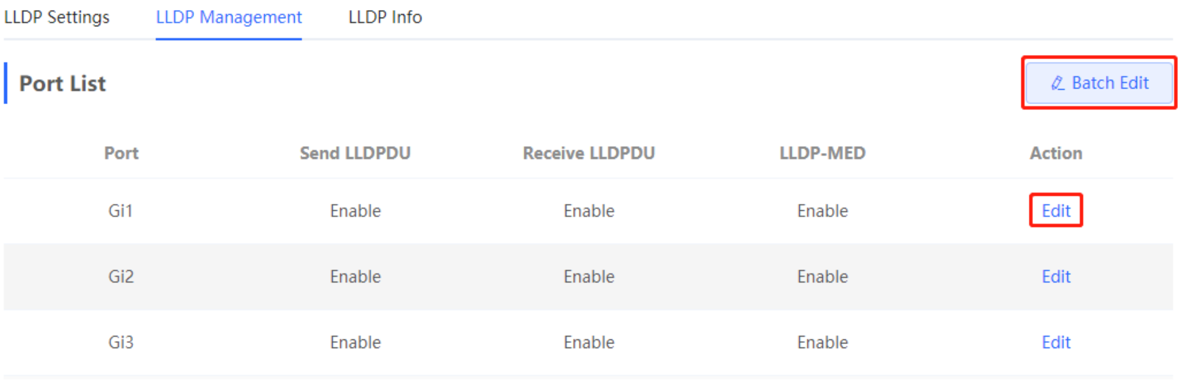
Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Management**.

In **Port List**, Click **Edit** in the **Action** column, or click **Batch Edit**, select the desired port, configure the LLDP working mode on the port and whether to enable LLDP-MED, and click **OK**.

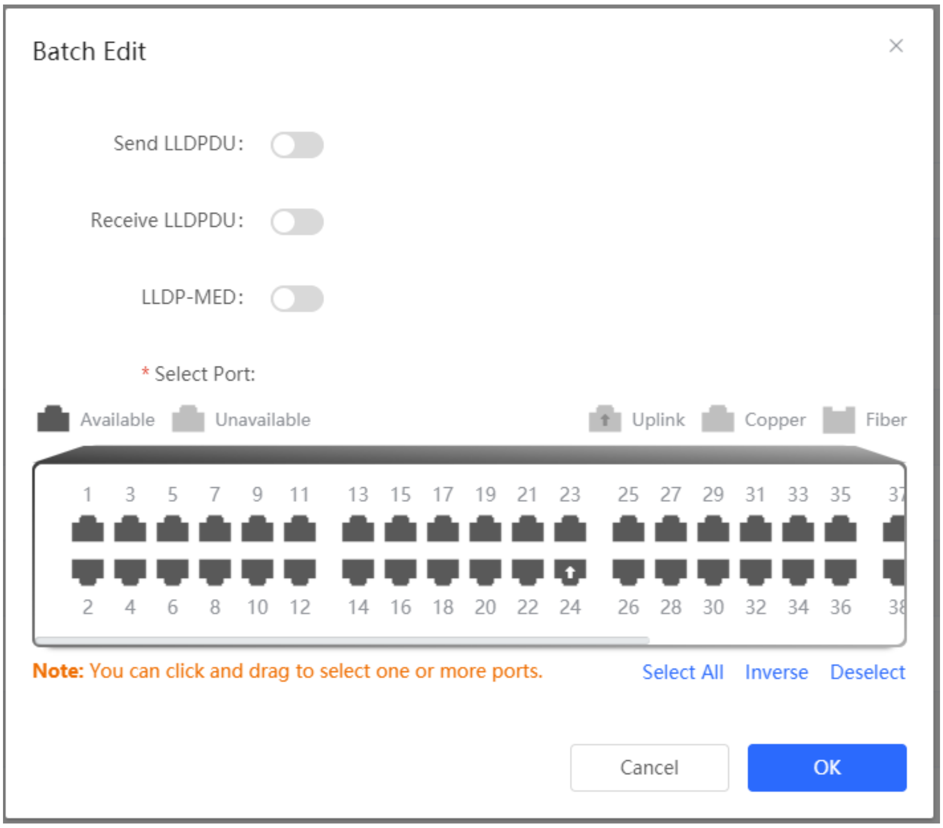
Send LLDPDU: After **Send LLDPDU** is enabled on a port, the port can send LLDPDUs.

Receive LLDPDU: After **Receive LLDPDU** is enabled on a port, the port can receive LLDPDUs.

LLDPMED: After **LLDPMED** is enabled, the device is capable of discovering neighbors when its peer endpoint supports LLDP-MED (the Link Layer Discovery Protocol-Media Endpoint Discovery).



Port	Send LLDPDU	Receive LLDPDU	LLDP-MED	Action
Gi1	Enable	Enable	Enable	Edit
Gi2	Enable	Enable	Enable	Edit
Gi3	Enable	Enable	Enable	Edit



Batch Edit

Send LLDPDU:

Receive LLDPDU:

LLDP-MED:

* Select Port:

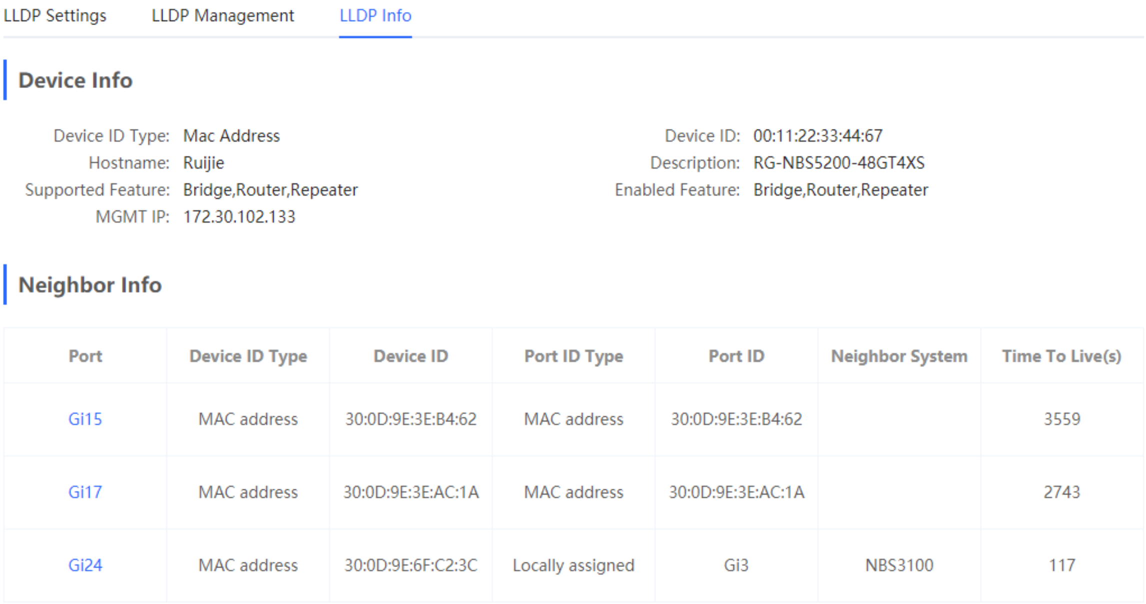
Note: You can click and drag to select one or more ports.

16.2.4 Displaying LLDP information

Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Info**.

To display LLDP information, including Including the LLDP information of the local device and the neighbor devices of each port. Click the port name to display details about port neighbors.

You can check the topology connection through LLDP information, or use LLDP to detect errors. For example, if two switch devices are directly connected in the network topology. When an administrator configures the VLAN, port rate, duplex mode, an error will be prompted if the configurations do not match those on the connected neighbor.



Device Info

Device ID Type: Mac Address

Hostname: Ruijie

Supported Feature: Bridge,Router,Repeater

MGMT IP: 172.30.102.133

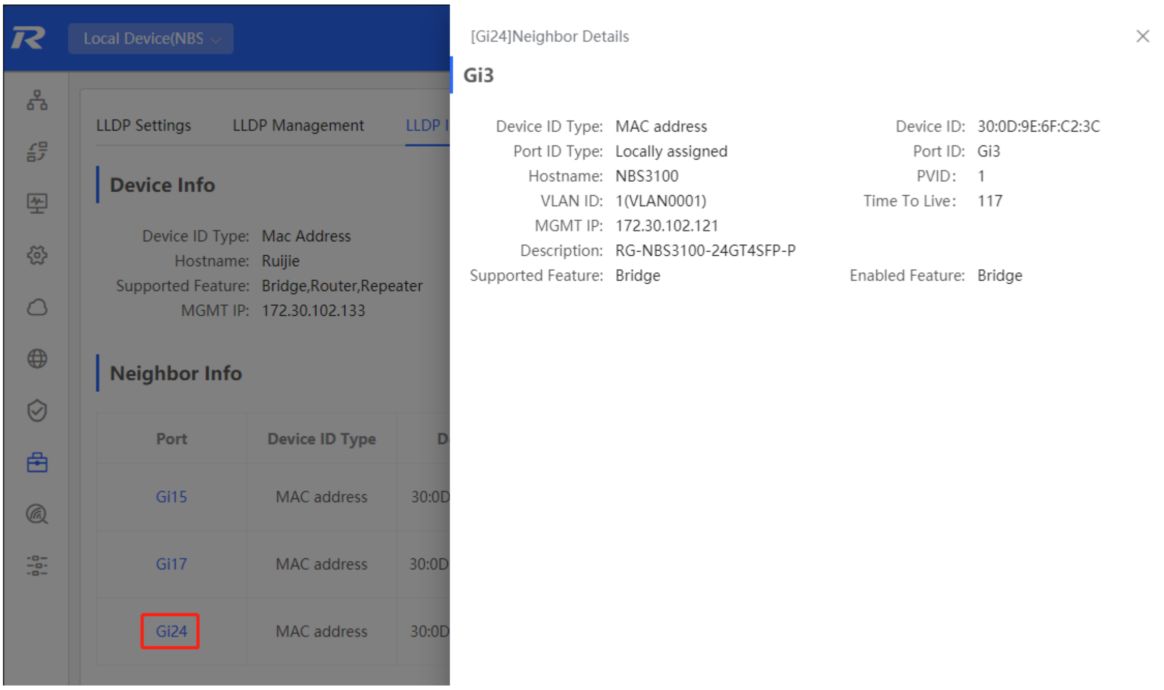
Device ID: 00:11:22:33:44:67

Description: RG-NBS5200-48GT4XS

Enabled Feature: Bridge,Router,Repeater

Neighbor Info

Port	Device ID Type	Device ID	Port ID Type	Port ID	Neighbor System	Time To Live(s)
Gi15	MAC address	30:0D:9E:3E:B4:62	MAC address	30:0D:9E:3E:B4:62		3559
Gi17	MAC address	30:0D:9E:3E:AC:1A	MAC address	30:0D:9E:3E:AC:1A		2743
Gi24	MAC address	30:0D:9E:6F:C2:3C	Locally assigned	Gi3	NBS3100	117



Local Device(NBS

LLDP Settings LLDP Management LLDP I

Device Info

Device ID Type: Mac Address
Hostname: Ruijie
Supported Feature: Bridge,Router,Repeater
MGMT IP: 172.30.102.133

Neighbor Info

Port	Device ID Type	D
Gi15	MAC address	30:0D
Gi17	MAC address	30:0D
Gi24	MAC address	30:0D

[Gi24]Neighbor Details

Gi3

Device ID Type: MAC address
Port ID Type: Locally assigned
Hostname: NBS3100
VLAN ID: 1(VLAN0001)
MGMT IP: 172.30.102.121
Description: RG-NBS3100-24GT4SFP-P
Supported Feature: Bridge
Device ID: 30:0D:9E:6F:C2:3C
Port ID: Gi3
PVID: 1
Time To Live: 117
Enabled Feature: Bridge

16.3 RLDP

16.3.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet L2 loops.

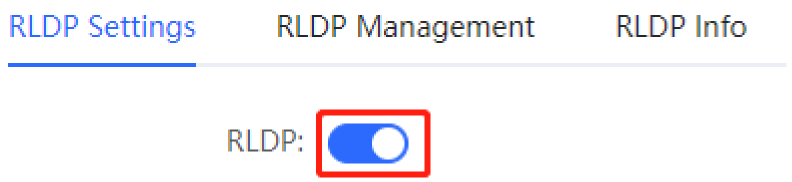
Supports enabling the RLDP function of the access switches in the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and the handling methods after a link fault is detected

16.3.2 Standalone Device Configuration

1. **RLDP Global Settings**

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Settings**.

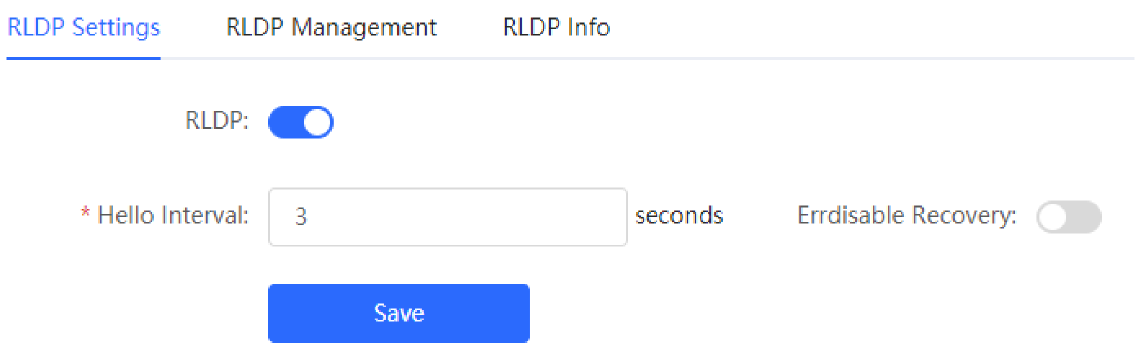
(1) Enable the RLDP function and click **OK** in the displayed dialog box. The RLDP function is disabled by default.



RLDP Settings RLDP Management RLDP Info

RLDP: ●

(2) Configure RLDP global parameters and click **Save**.



RLDP: ●

* Hello Interval: 3 seconds

Errdisable Recovery: ○

Table 8-4 Description of RLDP Global Configuration Parameters

Parameter	**Description**	**Default Value**
RLDP	Indicates whether the RLDP function is enabled.	Disable
Hello Interval	Interval for RLDP to send detection packets, in seconds	3 seconds
Errdisable Recovery	After it is enabled, a port automatically recovers to the initialized state after a loop occurs.	Disable
Errdisable Recovery Interval	The interval at which the failed ports recover to the initialized state regularly and link detection is restarted, in seconds.	30 seconds

2. Applying RLDP to a Port

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Management**.

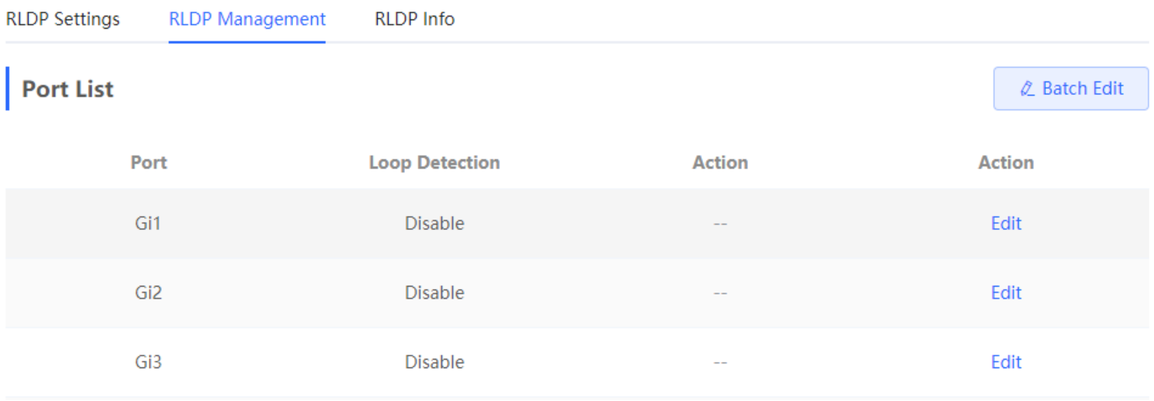
In **Port List,** click **Edit** in the Action column or click **Batch Edit**, select the desired port, configure whether to enable loop detection on the port and the handling method after a fault is detected, and click **OK**.

There are three methods to handle port failures:

- Warning: Only the relevant information is prompted to indicate the failed port and the failure type.
- Block: After alerting the fault, set the faulty port not to forward the received packets
- Shutdown port: After alerting the fault, shutdown the port.

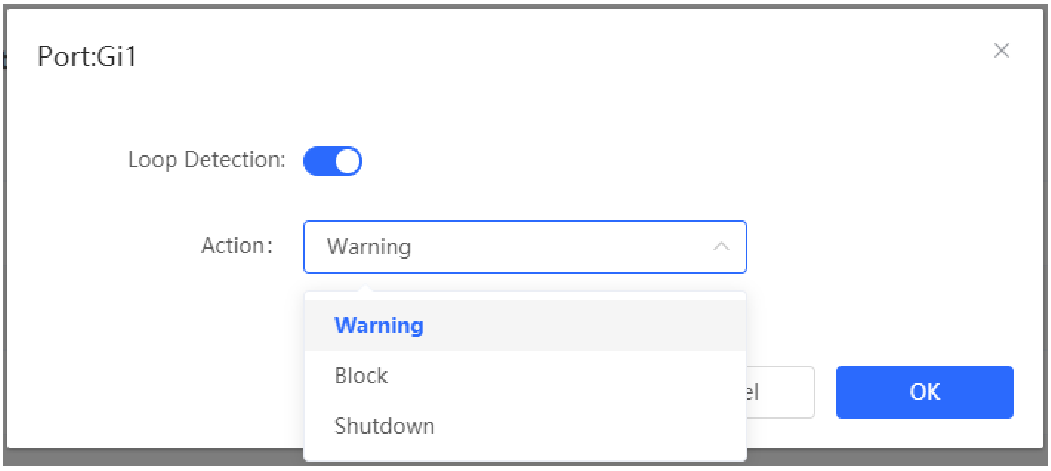
⚠ **Caution**

- When RLDP is applied to an aggregate port, the **Action** can only be set to **Warning** and **Shutdown**.
- When performing RLDP detection on an aggregate port, if detection packets are received on the same device, even if the VLANs of the port sending the packets and the port receiving them are different, it will not be judged as a loop failure.



Port List

Port	Loop Detection	Action	Action
Gi1	Disable	--	Edit
Gi2	Disable	--	Edit
Gi3	Disable	--	Edit



Port:Gi1

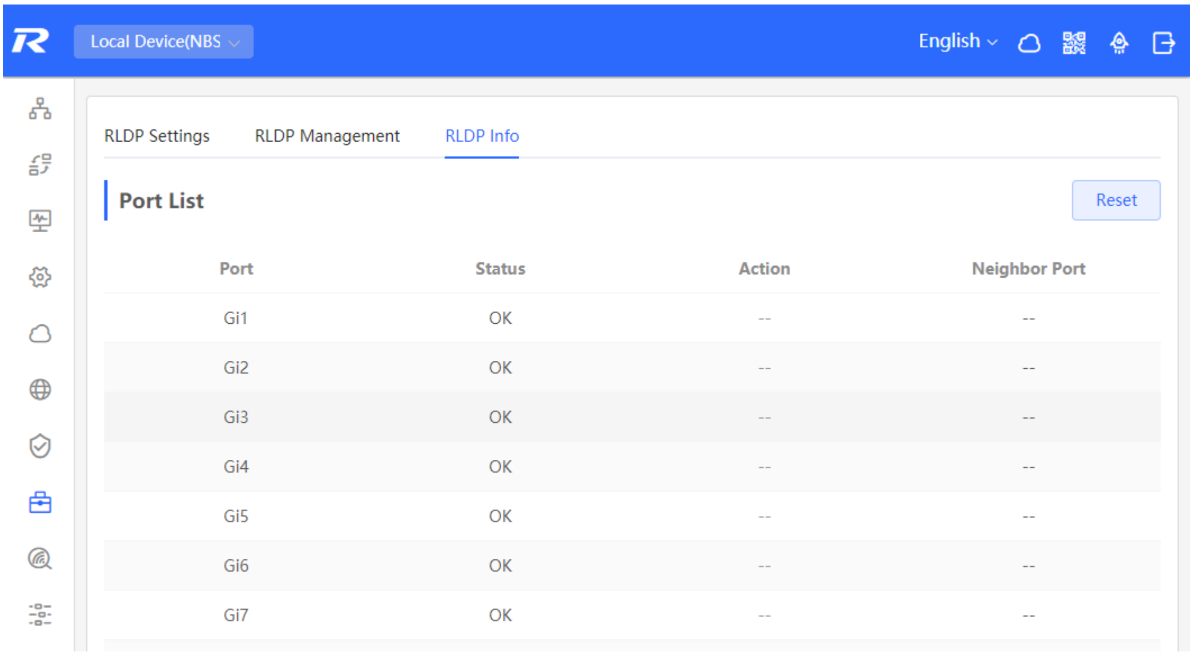
Loop Detection: on

Action: Warning

3. Displaying RLDP information

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Info**.

You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDP status triggered by a port to the normal state.



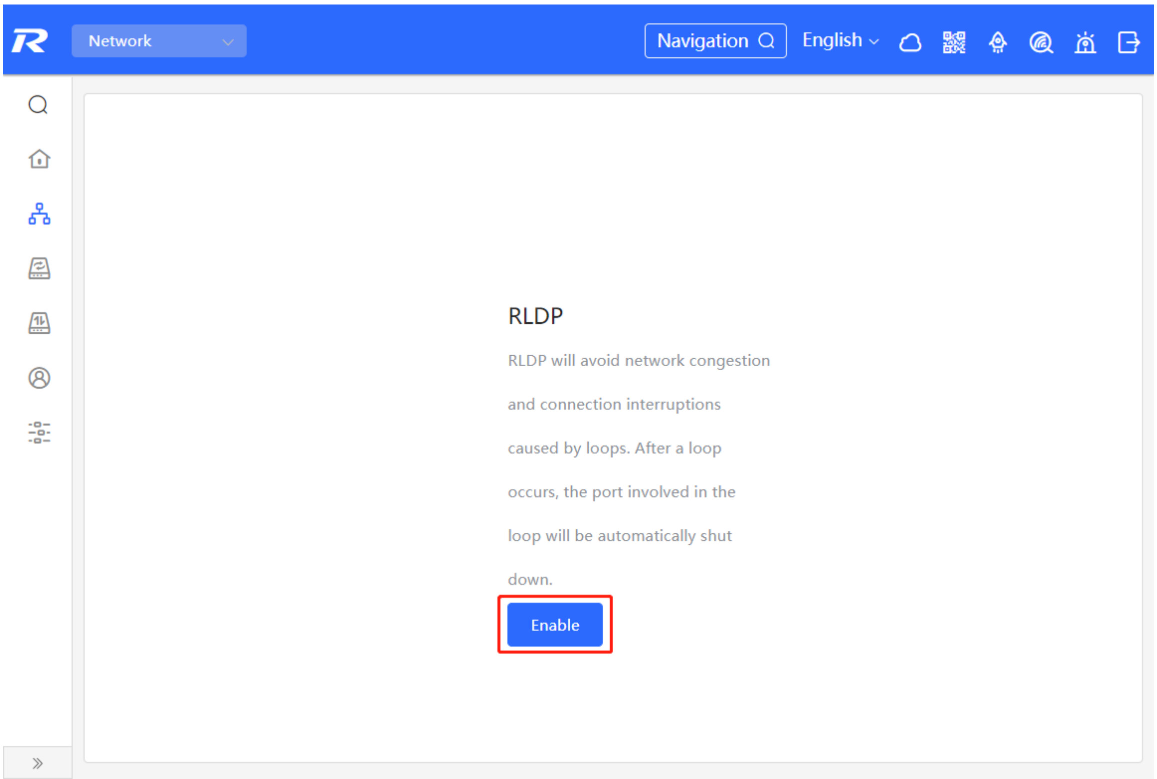
Port List

Port	Status	Action	Neighbor Port
Gi1	OK	--	--
Gi2	OK	--	--
Gi3	OK	--	--
Gi4	OK	--	--
Gi5	OK	--	--
Gi6	OK	--	--
Gi7	OK	--	--

16.3.3 Batch Configuring Network Switches

Choose **Network** > **RLDP**.

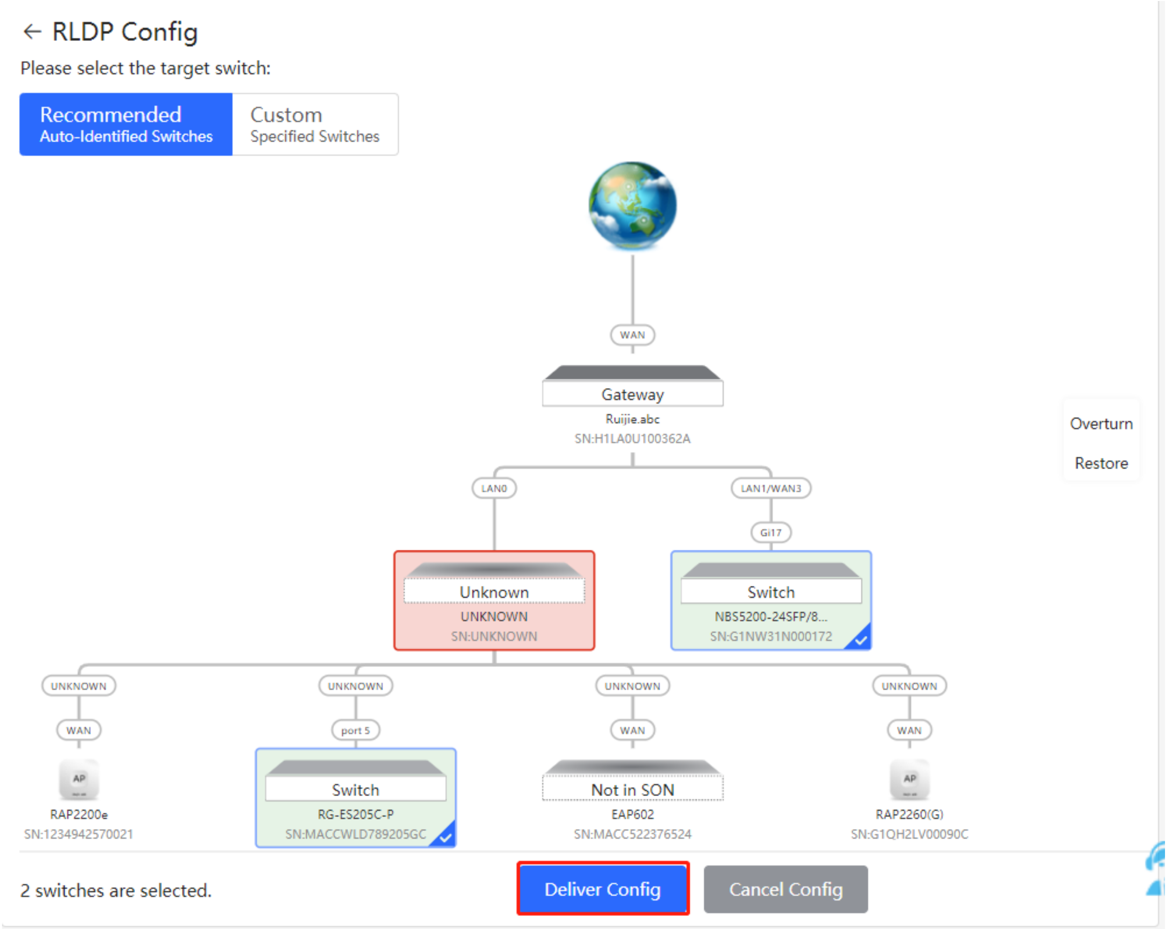
(1) Click **Enable** to access the **RLDP Config** page.



RLDP

RLDP will avoid network congestion and connection interruptions caused by loops. After a loop occurs, the port involved in the loop will be automatically shut down.

(2) In the networking topology, you can select the access switches on which you want to enable RLDP in either recommended or custom mode. If you select the recommended mode, all access switches in the network are selected automatically. If you select the custom mode, you can manually select the desired access switches. Click **Deliver Config**. RLDP is enabled on the selected switches.

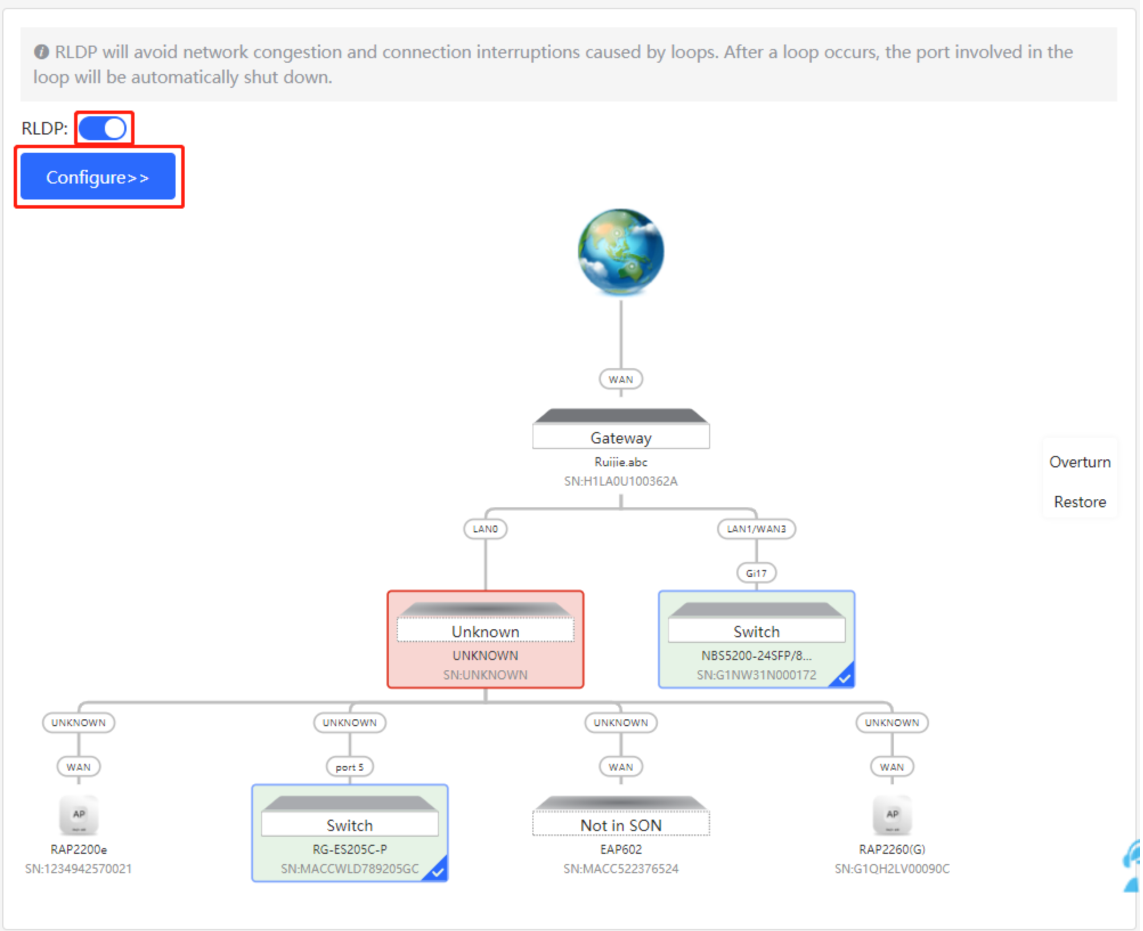


← RLDP Config

Please select the target switch:

2 switches are selected.

(3) After the configuration is delivered, if you want to modify the effective range of the RLDP function, click **Configure** to select desired switches in the topology again. Turn off **RLDP** to disable RLDP on all the switches with one click.



RLDP will avoid network congestion and connection interruptions caused by loops. After a loop occurs, the port involved in the loop will be automatically shut down.

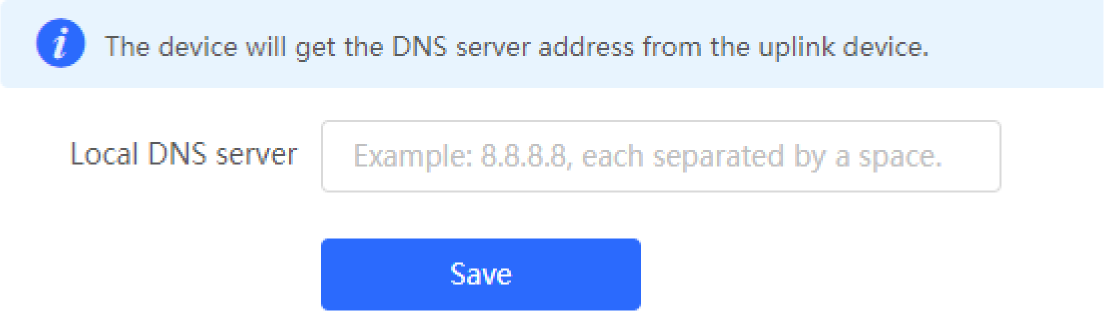
RLDP: ●

16.4 Configuring the Local DNS

The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default.

Choose **Local Device** > **Advanced** > **Local DNS**.

Enter the DNS server address used by the local device. If multiple addresses exist, separate them with spaces. Click **Save**. After configuring the local DNS, the device first use the DNS of the management IP address for parsing domain names. If the device fail to parse domain names, then use this DNS address instead.



The device will get the DNS server address from the uplink device.

Local DNS server: Example: 8.8.8.8, each separated by a space.

16.5 Voice VLAN

⚠ **Caution**

The Voice VLAN function is supported by RG-NBS3100 Series, RG-NBS3200 Series, RG-NBS5100 Series and RG-NBS5200 Series Switches.

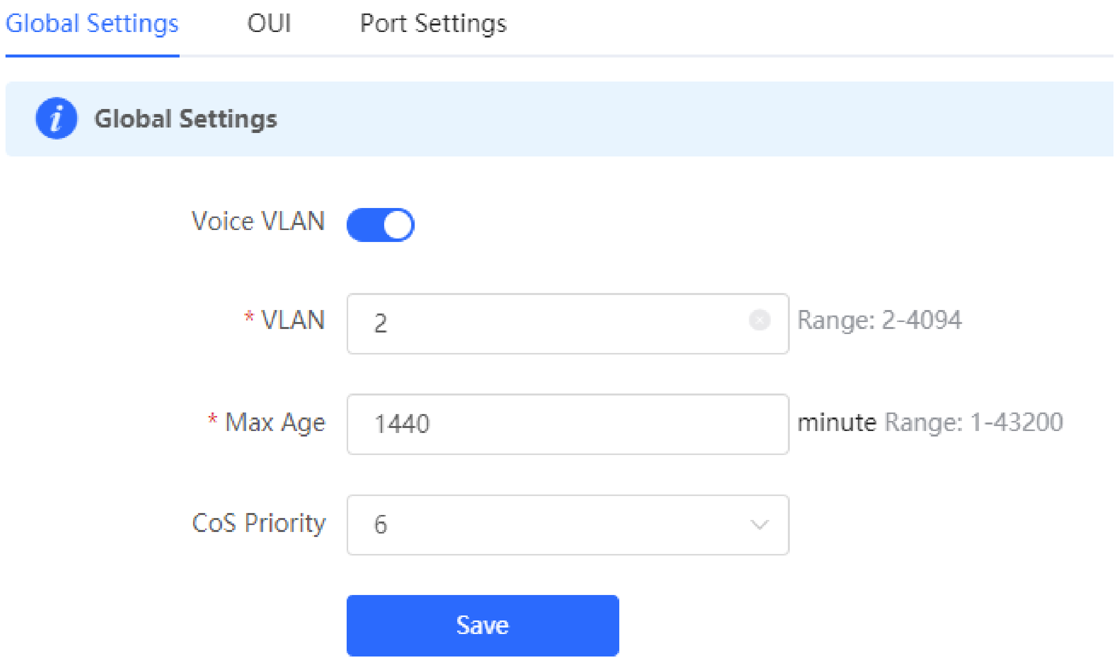
16.5.1 Overview

A voice virtual local area network (VLAN) is a VLAN dedicated to voice traffic of users. By creating a voice VLAN and adding ports connected to voice devices to the voice VLAN, you can have voice data transmitted in the voice VLAN and deliver specified policy of the quality of service (QoS) for voice streams, to improve the transmission priority of voice traffic and ensure the call quality.

16.5.2 Voice VLAN Global Configuration

Choose **Local Device** > **Advanced** > **Voice VLAN** > **Global Settings**.

Turn on the voice VLAN function, configure global parameters, and click **Save**.



Voice VLAN: ●

* VLAN: 2 Range: 2-4094

* Max Age: 1440 minute Range: 1-43200

CoS Priority: 6

Table 8-5 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable
VLAN	VLAN ID as Voice VLAN	NA

Parameter	Description	Default Value
Max Age	Aging time of voice VLAN, in minutes. In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN	1440 minutes
CoS Priority	The L2 Priority of voice stream packets in a Voice VLAN. The value range is from 0 to 7. A greater value indicates a higher priority. You can modify the priority of the voice traffic to improve the call quality.	6

16.5.3 Configuring a Voice VLAN OUI

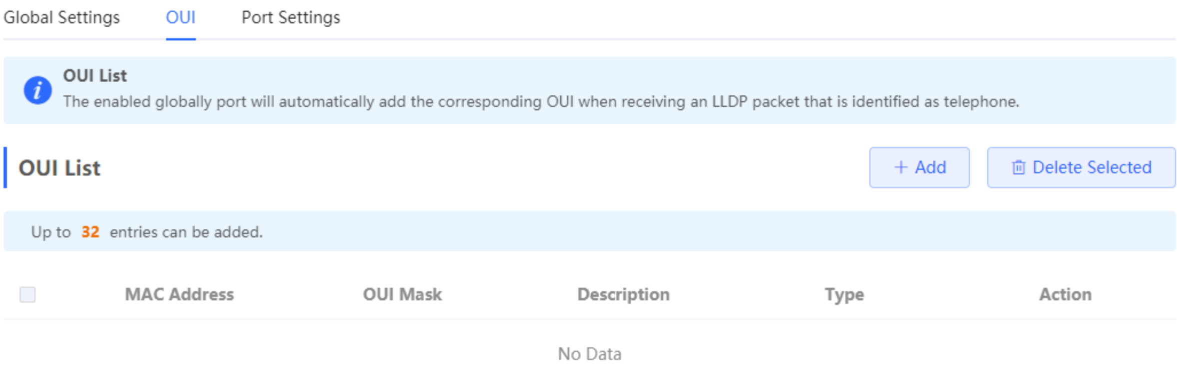
Choose **Local Device** > **Advanced** > **Voice VLAN** > **OUI**.

The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and sends them to the voice VLAN for transmission.

Note

After the voice VLAN function is enabled on a port, when the port receives LLDP packets sent by IP phones, it can identify the device capability fields in the packets, and identify the devices with the capability of **Telephone** as voice devices. It aslo extracts the source MAC address of a protocol packet and processes it as the MAC address of the voice device. In this way, the OUI can be added automatically.

Click **Add**. In the displayed dialog box, enter an MAC address and OUI, and click **OK**.



OUI List

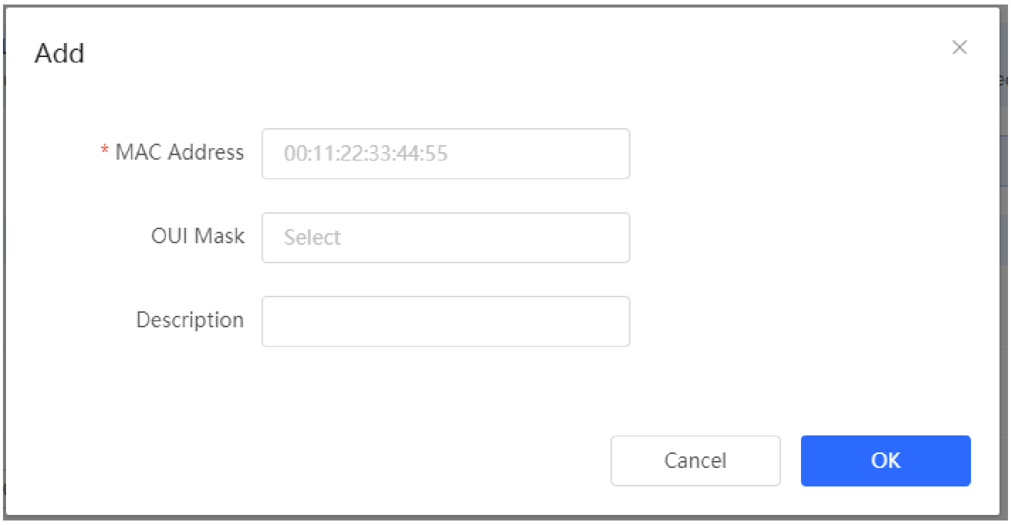
The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

OUI List

Up to 32 entries can be added.

□	MAC Address	OUI Mask	Description	Type	Action

No Data



Add

* MAC Address: 00:11:22:33:44:55

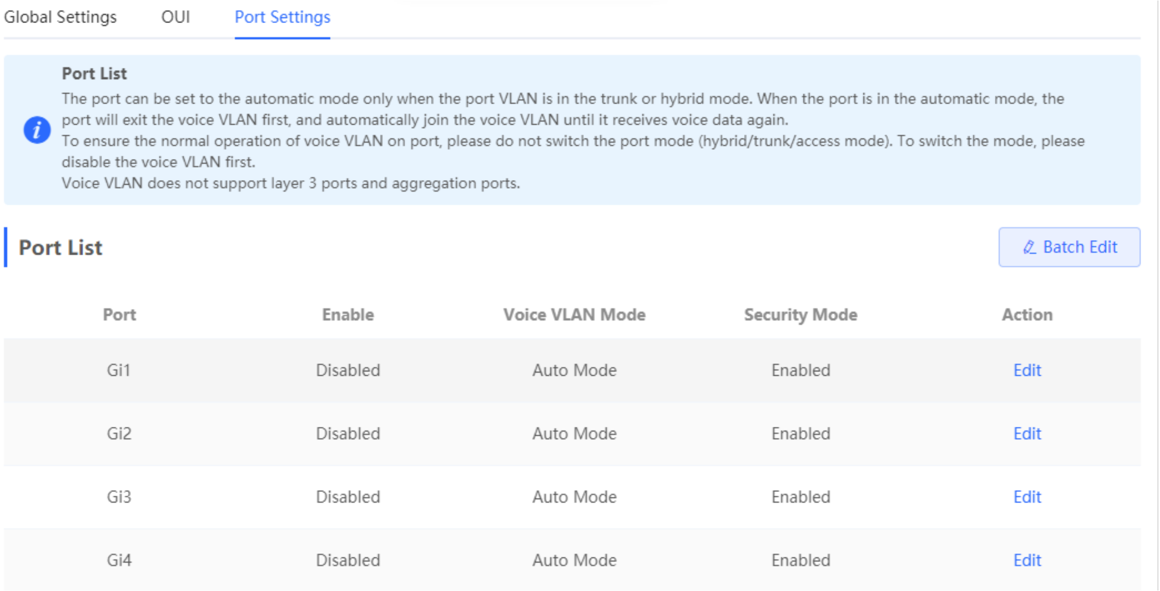
OUI Mask: Select

Description:

16.5.4 Configuring the Voice VLAN Function on a Port

Choose **Local Device** > **Advanced** > **Voice VLAN** > **Port Settings**.

Click **Edit** in the port entry or click **Batch Edit** on the upper -right corner. In the displayed dialog box, select whether to enable the voice VLAN function on the port, voice VLAN mode to be applied, and whether to enable the security mode, and Click **OK**.



Port List

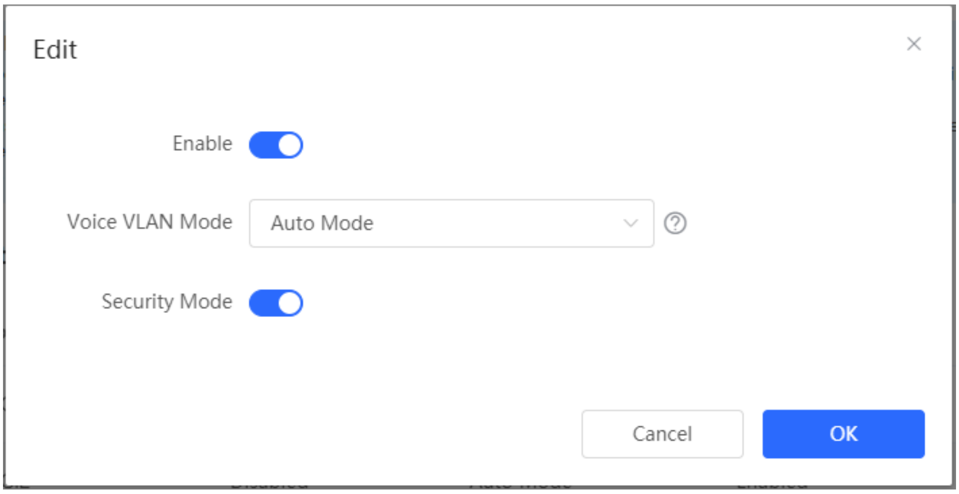
The port can be set to the automatic mode only when the port VLAN is in the trunk or hybrid mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

To ensure the normal operation of voice VLAN on port, please do not switch the port mode (hybrid/trunk/access mode). To switch the mode, please disable the voice VLAN first.

Voice VLAN does not support layer 3 ports and aggregation ports.

Port List

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Disabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit



Edit

Enable

Voice VLAN Mode: Auto Mode

Security Mode

Table 8-6 Description of the Voice VLAN Configuration Parameters on a Port

Parameter	Description	Default Value
Voice VLAN Mode	Based on different ways the Voice VLAN function is enabled on the port, the Voice VLAN Mode can be Auto Mode or Manual Mode: Auto Mode: In this mode, the device checks whether the permit VLANs of a port contain the voice VLAN after the voice VLAN function is enabled on the port. If yes, the device deletes the voice VLAN from the permit VLANs of the port until the port receives a voice packet containing a specified OUI. Then, the device automatically adds the voice VLAN to the port's permit VLANs. If the port does not receive a voice packet containing the specified OUI within the global aging time, the device removes the Voice VLAN from the permit VLANs of the port. Manual Mode: If the permit VLANs of a port contains the voice VLAN, voice packets can be transmitted in the voice VLAN.	Auto Mode
Security Mode	When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet. When the security mode is disabled, the source MAC addresses of packets are not checked and all packets can be transmitted in the voice VLAN.	Enable

Caution

- The voice VLAN mode of the port can be set as the auto mode only when the VLAN mode of the port is Trunk mode. When the voice VLAN mode of the port work in the auto mode, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.
- After the voice VLAN function is enabled on a port, do not switch the L2 mode (trunk or access mode) of the port to ensure normal operation of the function. If you need to switch the L2 mode of the port, disable the voice VLAN function on the port first.

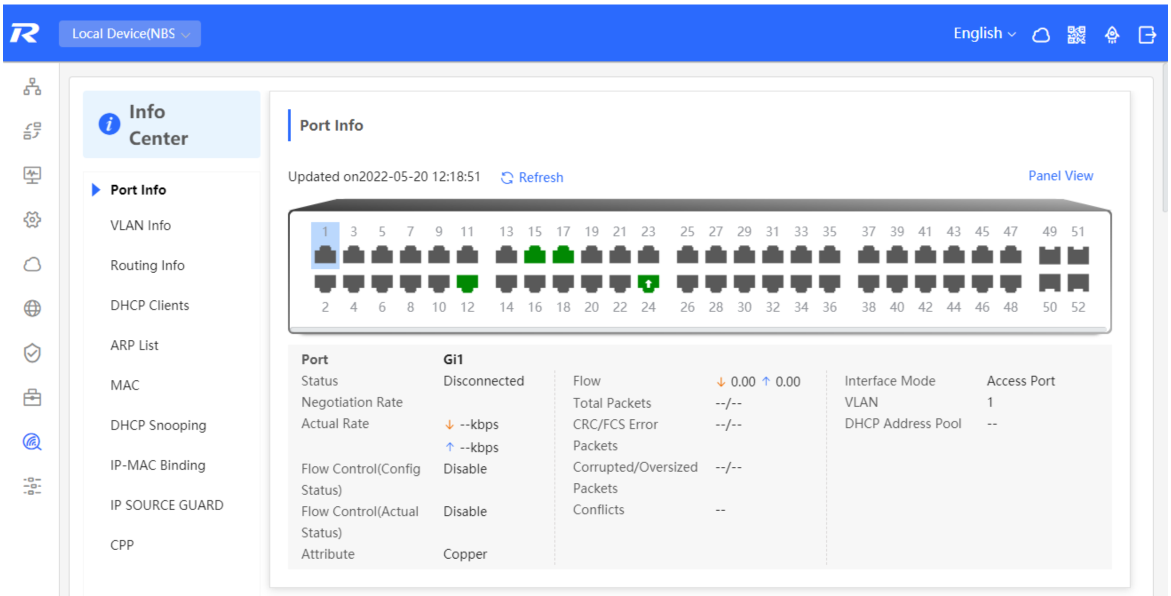
- It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.
- The voice VLAN function is unavailable on L3 ports or aggregate ports.

17 NBS Series Diagnostics

17.1 Info Center

Choose **Local Device** > **Diagnostics** > **Info Center**.

In **Info Center**, you can view port traffic, VLAN information, routing information, client list, ARP list, MAC address, DHCP snooping , IP-MAC binding, IP Source Guard, and CPP statistics of the device and relevant configurations.



Port Info

Updated on2022-05-20 12:18:51

Port	Gi1				
Status	Disconnected	Flow	↓ 0.00 ↑ 0.00	Interface Mode	Access Port
Negotiation Rate		Total Packets	--/--	VLAN	1
Actual Rate	↓ --kbps ↑ --kbps	CRC/FCS Error Packets	--/--	DHCP Address Pool	--
Flow Control(Config Status)	Disable	Corrupted/Oversized Packets	--/--		
Flow Control(Actual Status)	Disable	Conflicts	--		
Attribute	Copper				

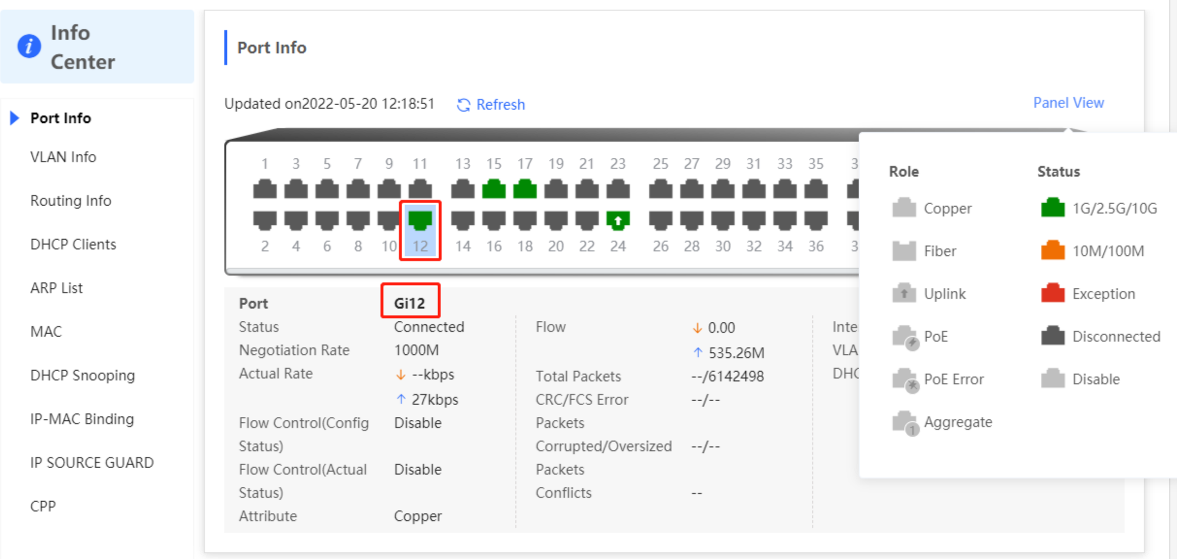
17.1.1 Port Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **Port Info**.

Port Info displays the status and configuration information of the port. Click the port icon to view the detailed information of the port.

Note

- To configure the flow control of the port or the optical/electrical attribute of a combo port, see 4.2.
- To configure the L2 mode of the port and the VLAN to which it belongs, see 3.5.3.



Updated on2022-05-20 12:18:51

Port	Gi12		
Status	Connected	Flow	↓ 0.00 ↑ 535.26M
Negotiation Rate	1000M		
Actual Rate	↓ --kbps ↑ 27kbps	Total Packets	--/6142498
		CRC/FCS Error Packets	--/--
Flow Control(Config Status)	Disable	Corrupted/Oversized Packets	--/--
Flow Control(Actual Status)	Disable	Conflicts	--
Attribute	Copper		

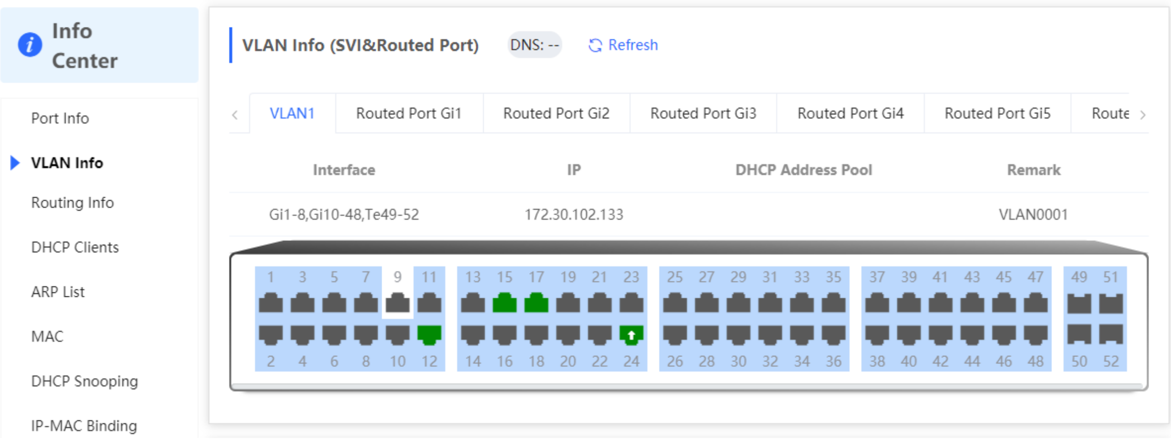
17.1.2 VLAN Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **VLAN Info**.

Display SVI port and routed port information, including the port information included in the VLAN, the port IP address, and whether the DHCP address pool is enabled.

Note

- To configure VLAN, see 11.5 .
- To configure SVI ports and routed ports, see 6.1.



Interface	IP	DHCP Address Pool	Remark
Gi1-8,Gi10-48,Te49-52	172.30.102.133		VLAN0001

17.1.3 Routing Info

Caution

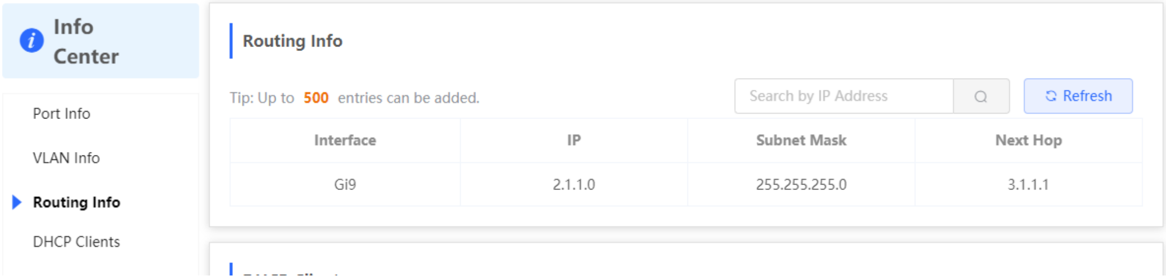
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

Choose **Local Device** > **Diagnostics** > **Info Center** > **Routing Info**.

Displays the routing information on the device. The search box in the upper-right corner supports finding route entries based on IP addresses.

Note

To set up static routes, see 6.3.



Routing Info

Tip: Up to 500 entries can be added.

Interface	IP	Subnet Mask	Next Hop
Gi9	2.1.1.0	255.255.255.0	3.1.1.1

17.1.4 DHCP Clients

Caution

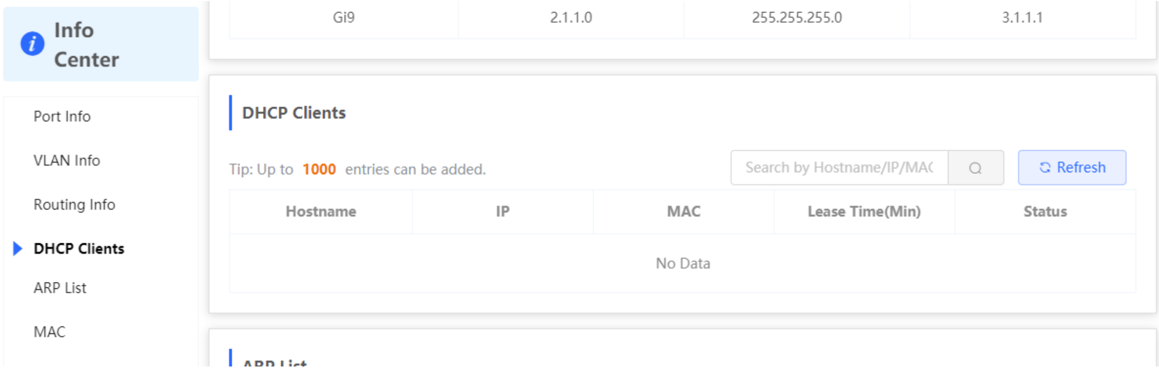
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Clients**.

Displays the IP address information assigned to endpoints by the device as a DHCP server.

Note

To configure DHCP server related functions, see 6.2.



Gi9	2.1.1.0	255.255.255.0	3.1.1.1

DHCP Clients

Tip: Up to 1000 entries can be added.

Hostname	IP	MAC	Lease Time(Min)	Status
No Data				

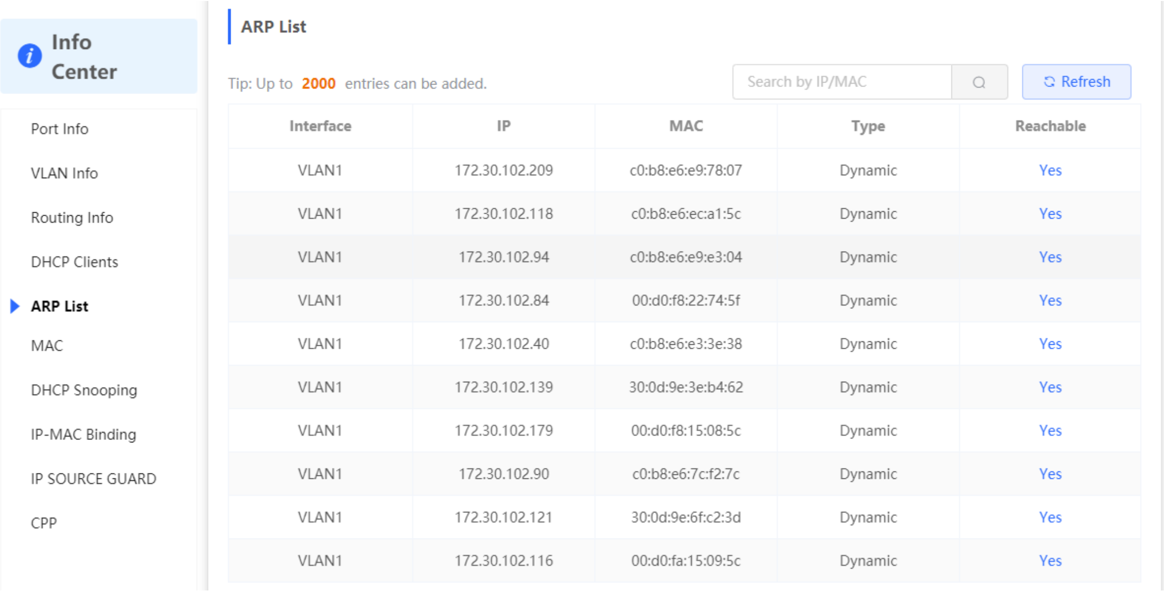
17.1.5 ARP List

Choose **Local Device** > **Diagnostics** > **Info Center** > **ARP List**.

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

Note

To bind dynamic ARP or manually configure static ARP, see 6.4.



Tip: Up to 2000 entries can be added.

Interface	IP	MAC	Type	Reachable
VLAN1	172.30.102.209	c0:b8:e6:e9:78:07	Dynamic	Yes
VLAN1	172.30.102.118	c0:b8:e6:ec:a1:5c	Dynamic	Yes
VLAN1	172.30.102.94	c0:b8:e6:e9:e3:04	Dynamic	Yes
VLAN1	172.30.102.84	00:d0:f8:22:74:5f	Dynamic	Yes
VLAN1	172.30.102.40	c0:b8:e6:e3:3e:38	Dynamic	Yes
VLAN1	172.30.102.139	30:0d:9e:3e:b4:62	Dynamic	Yes
VLAN1	172.30.102.179	00:d0:f8:15:08:5c	Dynamic	Yes
VLAN1	172.30.102.90	c0:b8:e6:7c:f2:7c	Dynamic	Yes
VLAN1	172.30.102.121	30:0d:9e:6f:c2:3d	Dynamic	Yes
VLAN1	172.30.102.116	00:d0:fa:15:09:5c	Dynamic	Yes

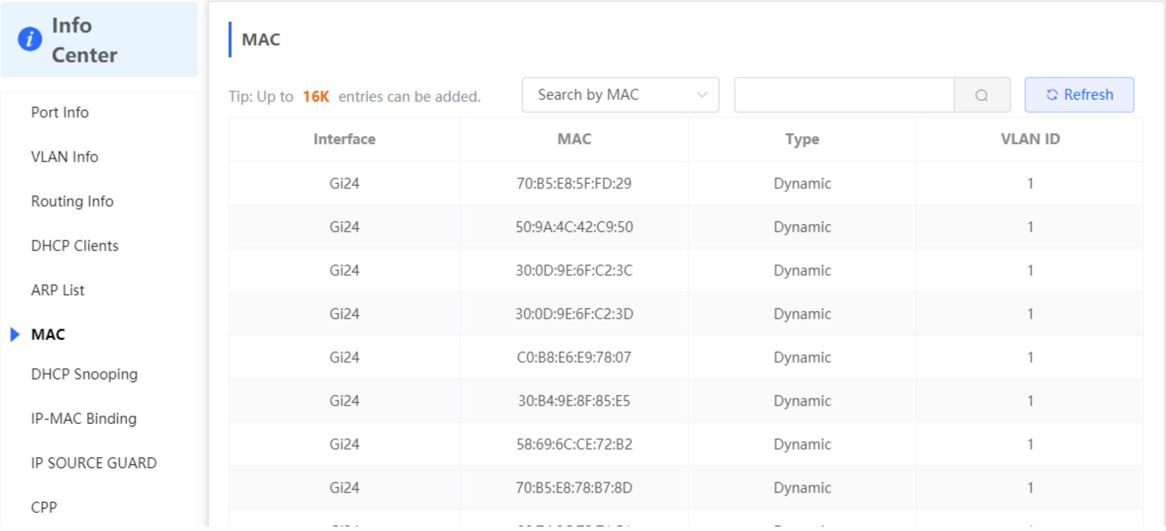
17.1.6 MAC Address

Choose **Local Device** > **Diagnostics** > **Info Center** > **MAC**.

Displays the MAC address information of the device, including the static MAC address manually configured by the user, the filtering MAC address, and the dynamic MAC address automatically learned by the device.

Note

To configure and manage the MAC address, see 3.3.



Tip: Up to 16K entries can be added.

Interface	MAC	Type	VLAN ID
Gi24	70:B5:E8:5F:FD:29	Dynamic	1
Gi24	50:9A:4C:42:C9:50	Dynamic	1
Gi24	30:0D:9E:6F:C2:3C	Dynamic	1
Gi24	30:0D:9E:6F:C2:3D	Dynamic	1
Gi24	C0:B8:E6:E9:78:07	Dynamic	1
Gi24	30:B4:9E:8F:85:E5	Dynamic	1
Gi24	58:69:6C:CE:72:B2	Dynamic	1
Gi24	70:B5:E8:78:B7:8D	Dynamic	1

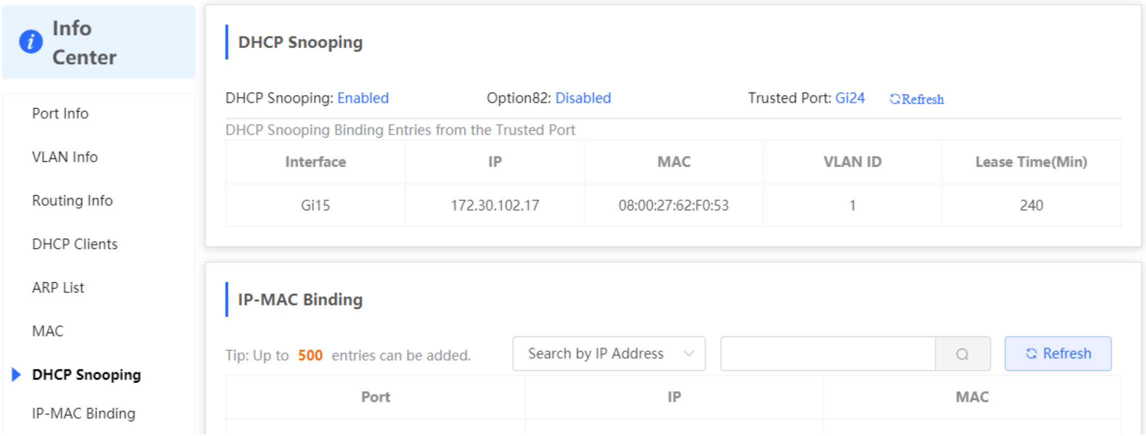
17.1.7 DHCP Snooping

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Snooping**.

Displays the current configuration of the DHCP snooping function and the user information dynamically learned by the trust port.

Note

To modify DHCP Snooping related configuration, see 7.1.



DHCP Snooping

DHCP Snooping: Enabled Option82: Disabled Trusted Port: Gi24

DHCP Snooping Binding Entries from the Trusted Port

Interface	IP	MAC	VLAN ID	Lease Time(Min)
Gi15	172.30.102.17	08:00:27:62:F0:53	1	240

IP-MAC Binding

Tip: Up to 500 entries can be added.

Port	IP	MAC

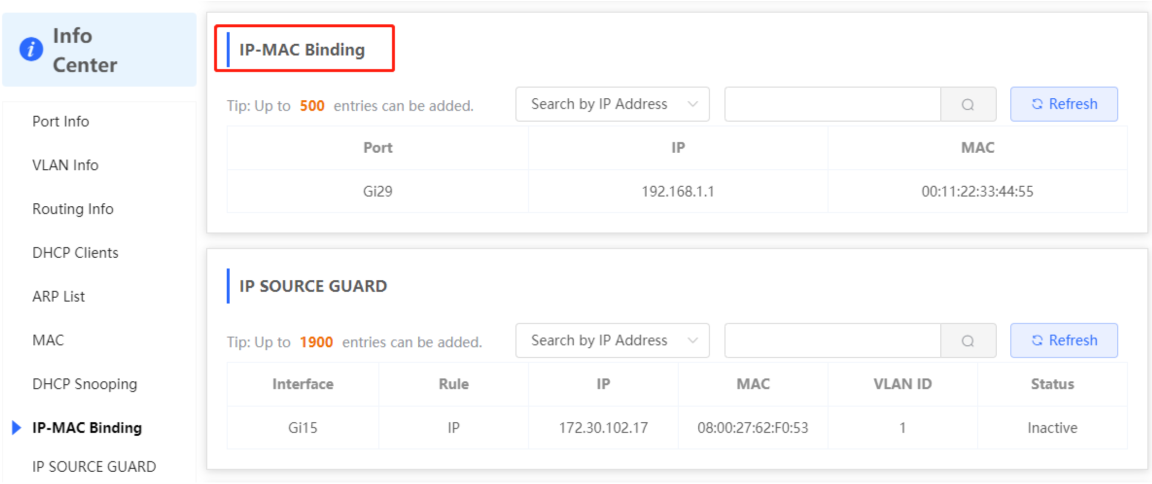
17.1.8 IP-MAC Binding

Choose **Local Device** > **Diagnostics** > **Info Center** > **IP-MAC Binding**.

Displays the configured IP-MAC binding entries. The device checks whether the source IP addresses and source MAC addresses of IP packets match those configured for the device and filters out IP packets not matching the binding.

Note

To add or modify the IP-MAC binding, see 7.5.



IP-MAC Binding

Tip: Up to 500 entries can be added.

Port	IP	MAC
Gi29	192.168.1.1	00:11:22:33:44:55

IP SOURCE GUARD

Tip: Up to 1900 entries can be added.

Interface	Rule	IP	MAC	VLAN ID	Status
Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive

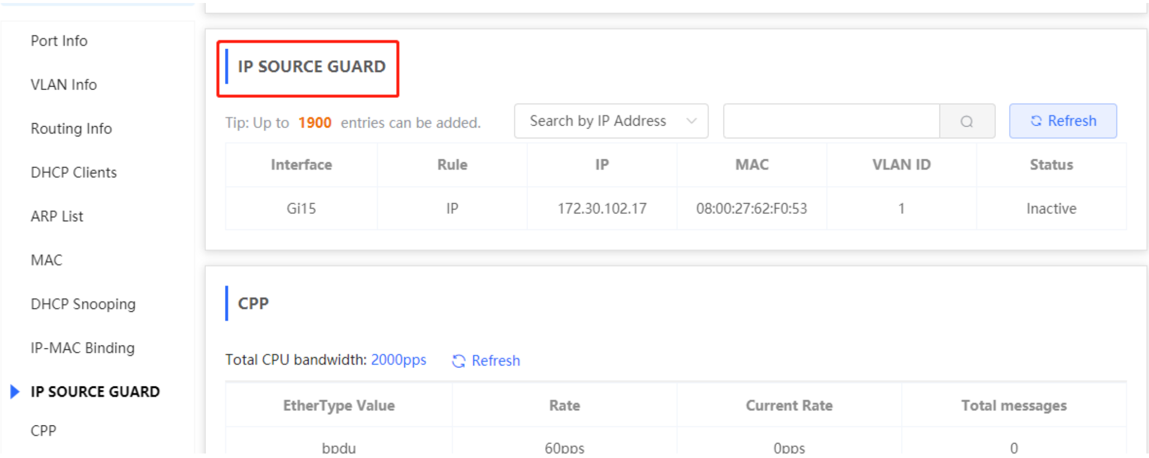
17.1.9 IP Source Guard

Choose **Local Device** > **Diagnostics** > **Info Center** > **Source Guard**.

Displays the binding list of the IP Source Guard function. The IP Source Guard function will check the IP packets from non-DHCP trusted ports according to the list, and filter out the IP packets that are not in the binding list.

Note

To configure IP Source Guard function, see 7.6.



IP SOURCE GUARD

Tip: Up to 1900 entries can be added.

Interface	Rule	IP	MAC	VLAN ID	Status
Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive

CPP

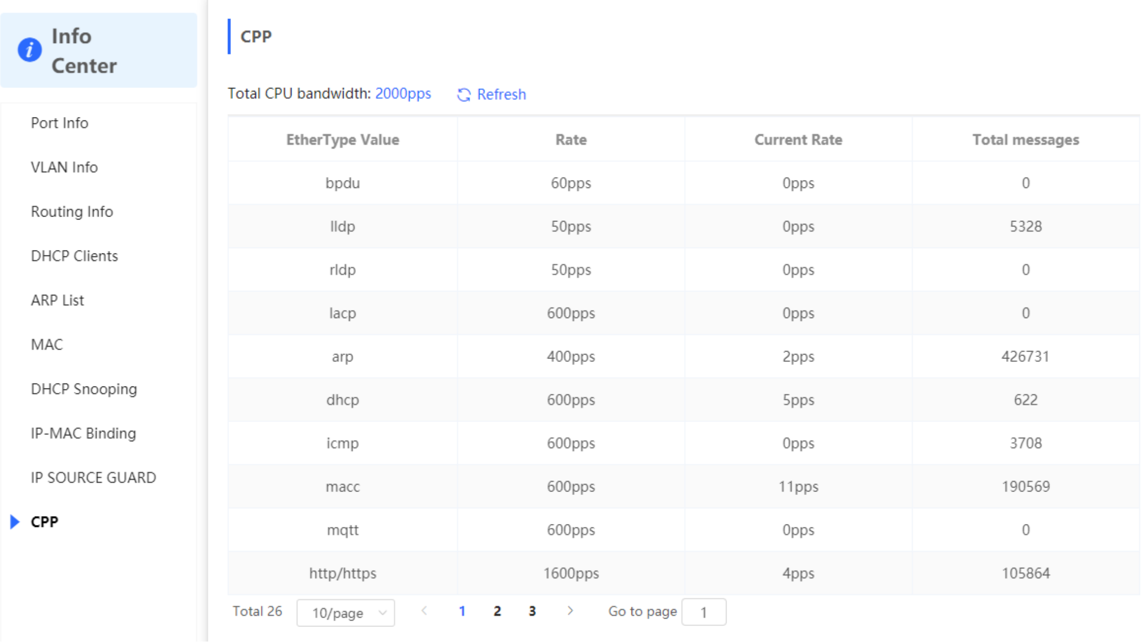
Total CPU bandwidth: 2000pps

EtherType Value	Rate	Current Rate	Total messages
bpdu	60pps	0pps	0

17.1.10 CPP Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **CPP**.

Displays the current total CPU bandwidth and statistics of various packet types, including the bandwidth, current rate, and total number of packets.



CPP

Total CPU bandwidth: 2000pps

EtherType Value	Rate	Current Rate	Total messages
bpdu	60pps	0pps	0
lldp	50pps	0pps	5328
rldp	50pps	0pps	0
lacp	600pps	0pps	0
arp	400pps	2pps	426731
dhcp	600pps	5pps	622
icmp	600pps	0pps	3708
macc	600pps	11pps	190569
mqtt	600pps	0pps	0
http/https	1600pps	4pps	105864

Total 26

17.2 Network Tools

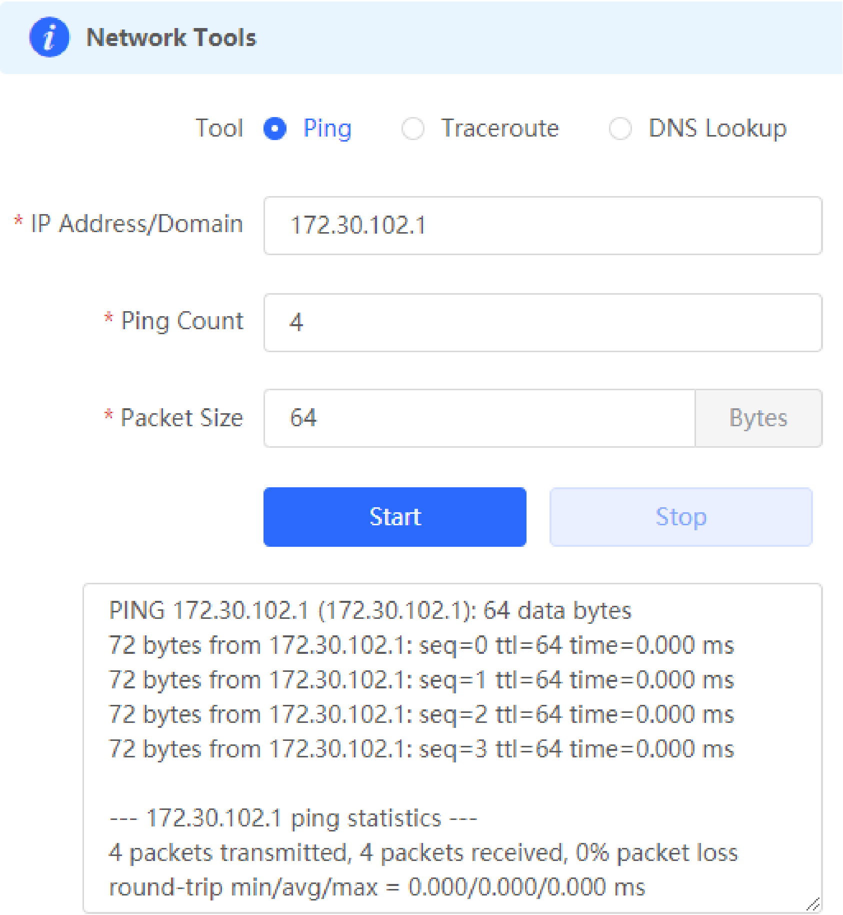
The **Network Tools** page provides three tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

17.2.1 Ping

Choose **Local Device** > **Diagnostics** > **Network Tools**.

The **Ping** command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, enter the destination IP address or website address, configure the ping count and packet size, and click **Start** to test the network connectivity between the device and the IP address or website. If "Ping failed" is displayed, the device is not reachable to the IP address or website.



Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 172.30.102.1

* Ping Count: 4

* Packet Size: 64 Bytes

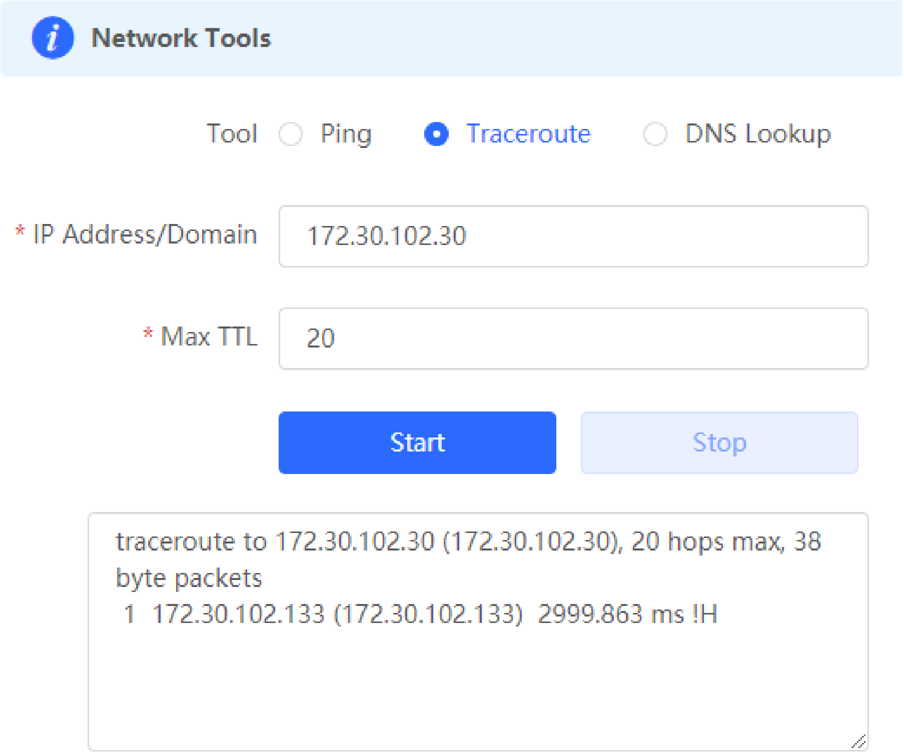
```
PING 172.30.102.1 (172.30.102.1): 64 data bytes
72 bytes from 172.30.102.1: seq=0 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=1 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=2 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=3 ttl=64 time=0.000 ms

--- 172.30.102.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

17.2.2 Traceroute

Choose **Local Device** > **Diagnostics** > **Network Tools**.

The **Traceroute** function is used to identify the network path from one device to another. On a simple network, the network path may pass through only one routing node or none at all. On a complex network, packets may pass through dozens of routing nodes before reaching their destination. The traceroute function can be used to judge the transmission path of data packets during communication.

Select **Traceroute** as the diagnosis mode, enter a destination IP address or the maximum TTL value used by the URL and traceroute, and click **Start**.



* IP Address/Domain: 172.30.102.30

* Max TTL: 20

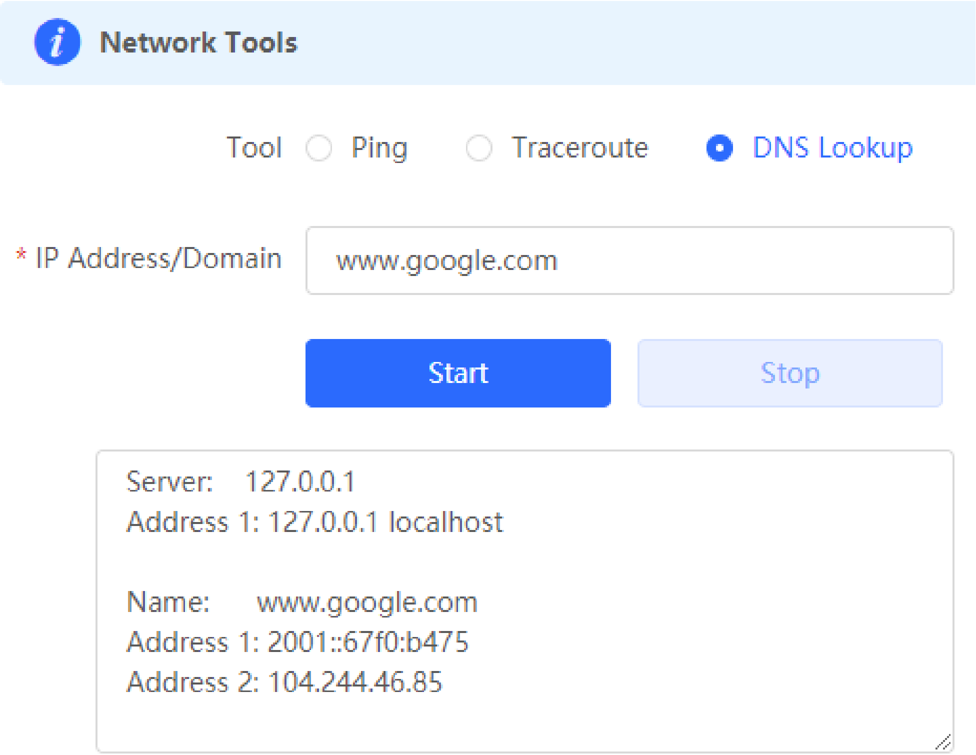
```
traceroute to 172.30.102.30 (172.30.102.30), 20 hops max, 38
byte packets
 1  172.30.102.133 (172.30.102.133)  2999.863 ms !H
```

17.2.3 DNS Lookup

Choose **Local Device** > **Diagnostics** > **Network Tools**.

DNS Lookup is used to query the information of network domain name or diagnose DNS server problems. If the device can ping through the IP address of the Internet from your web page but the browser cannot open the web page, you can use the DNS lookup function to check whether domain name resolution is normal.

Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and click **Start**.



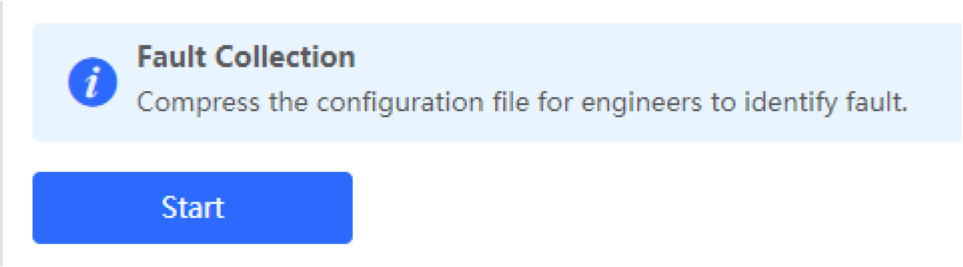
www.google.com

```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      www.google.com
Address 1: 2001::67f0:b475
Address 2: 104.244.46.85
```

17.3 Fault Collection

Choose **Local Device** > **Diagnostics** > **Fault Collection.**

When an unknown fault occurs on the device, you can collect fault information by one click on this page. Click **Start**. The configuration files of the device will be packed into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.

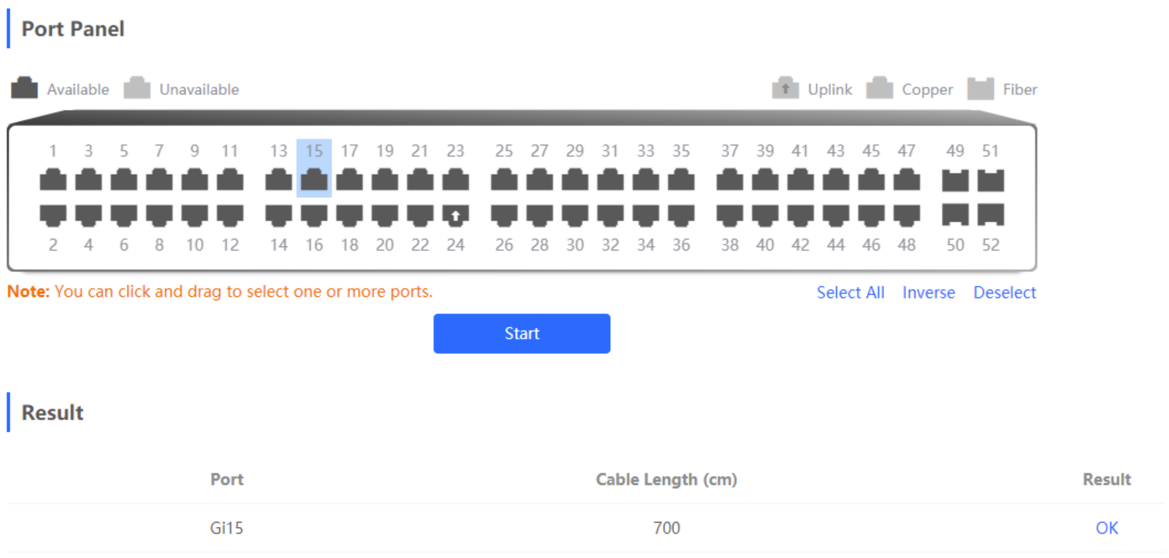

Fault Collection
Compress the configuration file for engineers to identify fault.
Start

17.4 Cable Diagnostics

Choose **Local Device** > **Diagnostics** > **Cable Diagnostics**.

The cable diagnostics function can detect the approximate length of a cable connected to a port and whether the cable is faulty.

Select the port to be detected on the port panel and click **Start**. The detection results will be displayed below.



Note: You can click and drag to select one or more ports.

Result

Port	Cable Length (cm)	Result
Gi15	700	OK

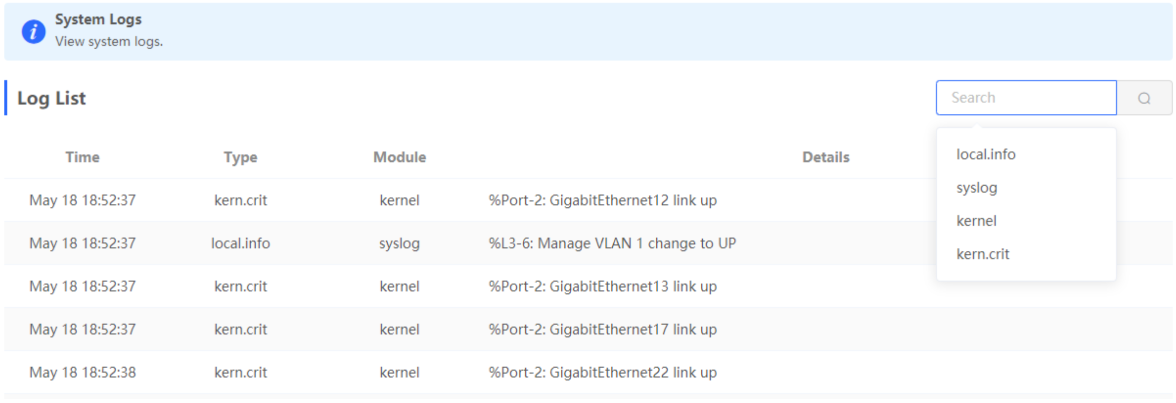
Caution

- The SPF port does not support the function.
- If a detected port contains an uplink port, the network may be intermittently disconnected. Exercise caution when performing this operation.

17.5 System Logs

Choose **Local Device** > **Diagnostics** > **System Logs**.

System logs record device operations, operation time, and operation modules. System logs are used by administrators to monitor the running status of the device, analyze network status, and locate faults. You can search for specified logs by fault type, faulty module, and keyword in fault information.



System Logs
View system logs.

Log List

Time	Type	Module	Details
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up
May 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet13 link up
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet17 link up
May 18 18:52:38	kern.crit	kernel	%Port-2: GigabitEthernet22 link up

17.6 Alerts

Choose **Local Device** > **Diagnostics** > **Alerts**.

Note

Choose **Network** > **Alerts** to view the alert information of other devices in the network.

Displays possible problems on the network environment to facilitate fault prevention and troubleshooting. You can view the alert occurrence time, port, alert impact, and handling suggestions, and rectify device faults according to handling suggestions.

All types of alerts are concerned by default. You can click **Unfollow** to unfollow this type of alert. The system will no longer display this type of alert. To enable the notification function of a type of alert again, follow the alert type on the **Removed Alert** page.

⚠ **Caution**

After unfollowing an alert, the system will not issue an alert prompt for this type of fault, and users cannot find and deal with the fault in time. Exercise caution when performing this operation.

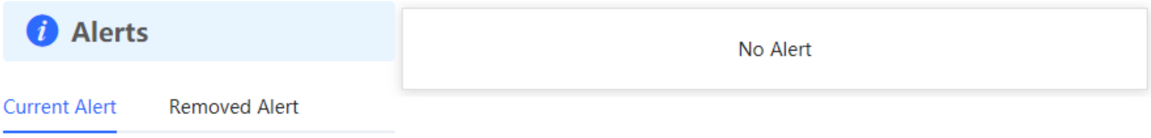


Table 9-1 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series, RG-NBS3200 Series Switches do not support this type of alert.
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	NA
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	NA
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of	NA

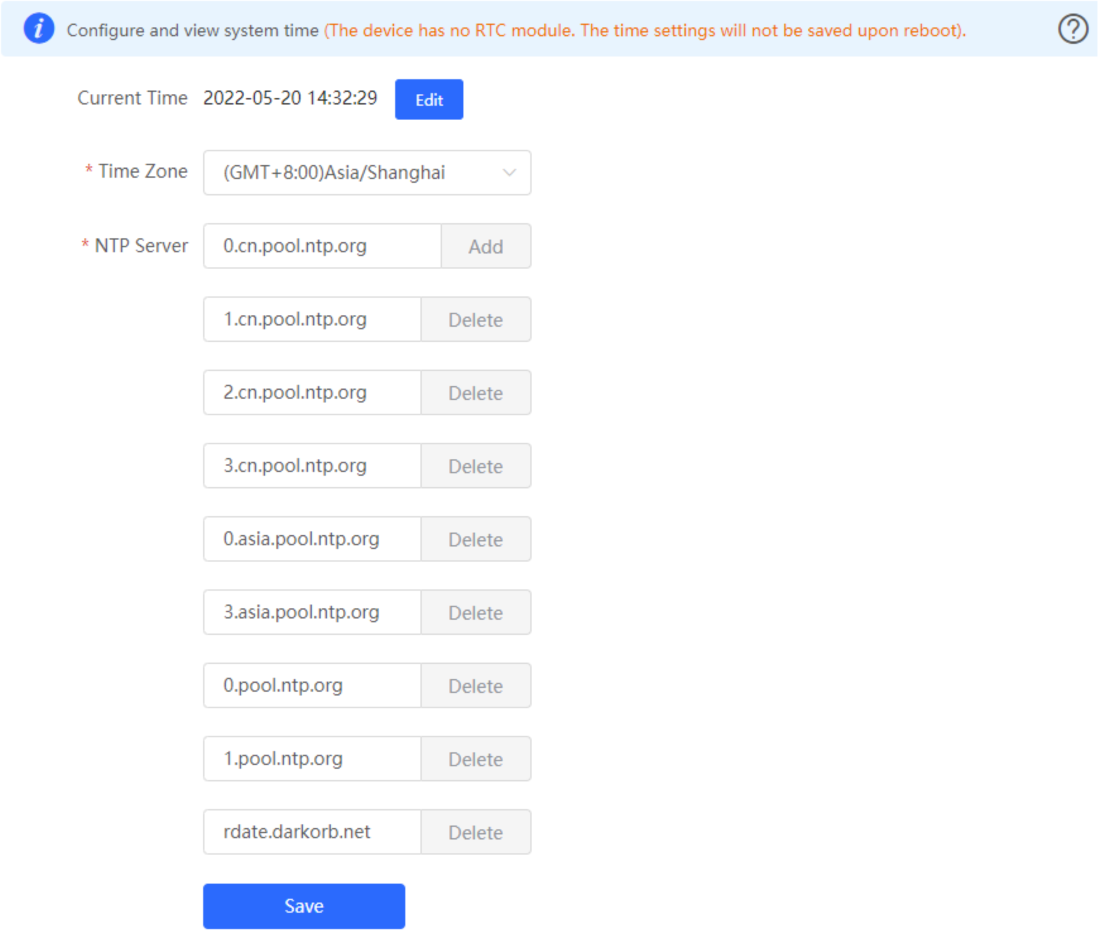
Alert Type	Description	Support Description
	the product.	
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	NA
The PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and the new connected PD cannot be powered properly.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	NA

18 NBS Series System Configuration

18.1 Setting the System Time

Choose **System** > **System Time**.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.



Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).

Current Time 2022-05-20 14:32:29

* Time Zone (GMT+8:00)Asia/Shanghai

* NTP Server 0.cn.pool.ntp.org

1.cn.pool.ntp.org

2.cn.pool.ntp.org

3.cn.pool.ntp.org

0.asia.pool.ntp.org

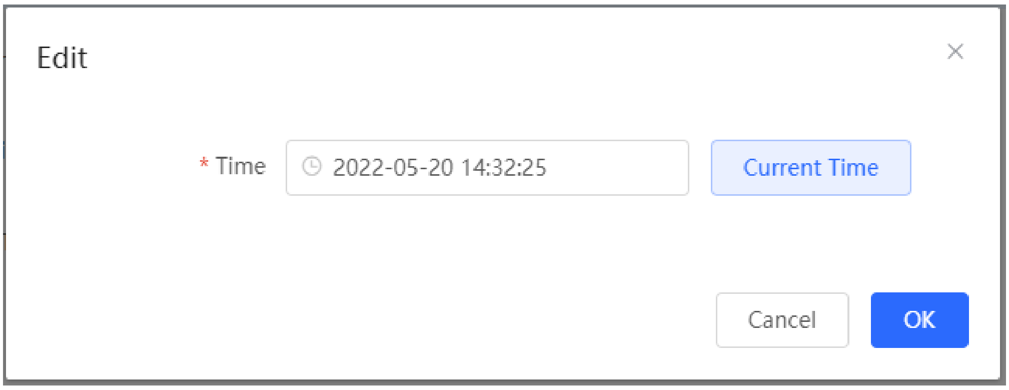
3.asia.pool.ntp.org

0.pool.ntp.org

1.pool.ntp.org

rdate.darkorb.net

Click **Current Time** when modifying the time, and the system time of the currently logged-in device will be automatically filled in.


Edit

* Time: 2022-05-20 14:32:25

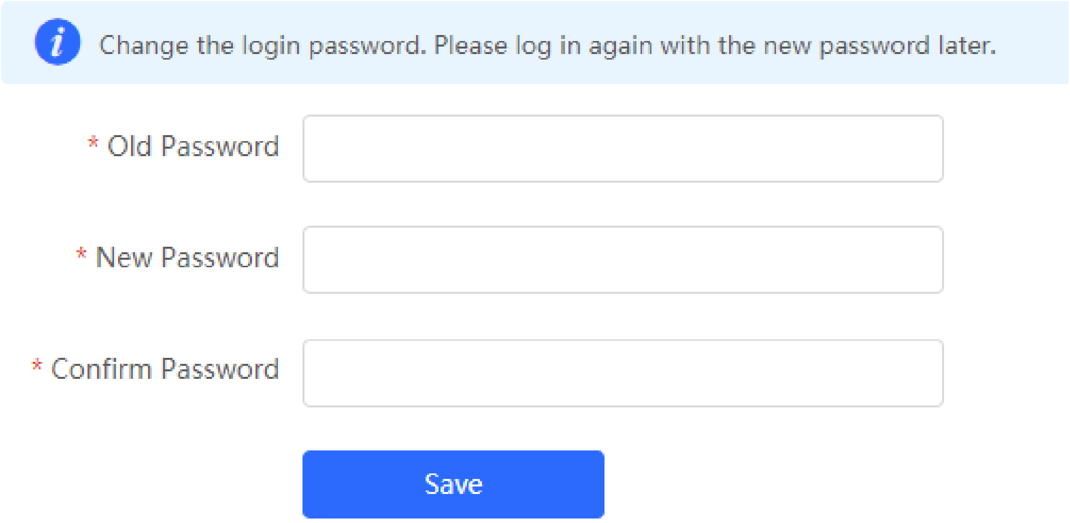
18.2 Setting the Web Login Password

Choose **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.


Change the login password. Please log in again with the new password later.

18.3 Setting the Session Timeout Duration

Choose **System** > **Login** > **Session Timeout**.

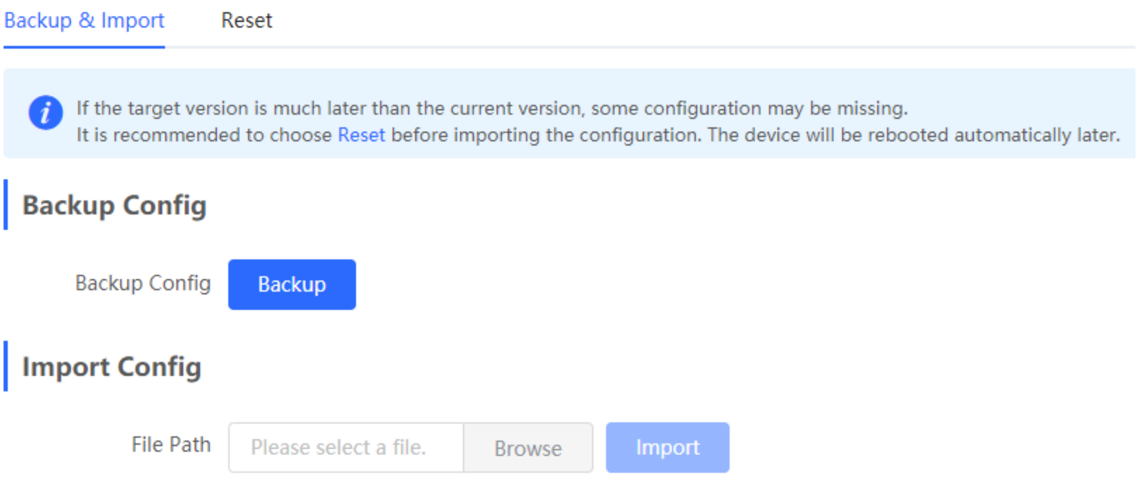
If you do not log out after login, the Eweb management system allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the Eweb management system automatically refreshes the page and you need to relog in before continuing your operations. You can change the session timeout duration.

18.4 Configuration Backup and Import

Choose **System** > **Management** > **Backup & Import**.

Configure backup: Click **Backup** to generate the backup configuration and download it locally.

Configure import: Click **Browse**, select a backup configuration file locally, and click **Import** to apply the configuration specified by the file to the device After importing the configuration, the device will restart.



If the target version is much later than the current version, some configuration may be missing.
It is recommended to choose Reset before importing the configuration. The device will be rebooted automatically later.

Backup Config

Backup Config

Import Config

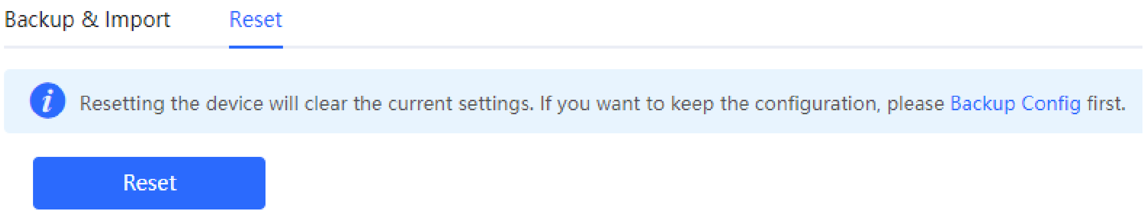
File Path: Please select a file.

18.5 Reset

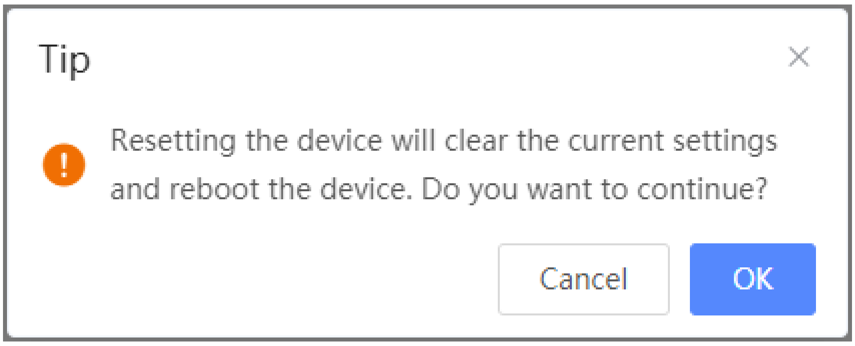
18.5.1 Resetting the Device

Choose **Local Device** > **System** > **Management** > **Reset**.

Click **Reset**, and click **OK** to restore factory settings.



Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.



Tip

Resetting the device will clear the current settings and reboot the device. Do you want to continue?

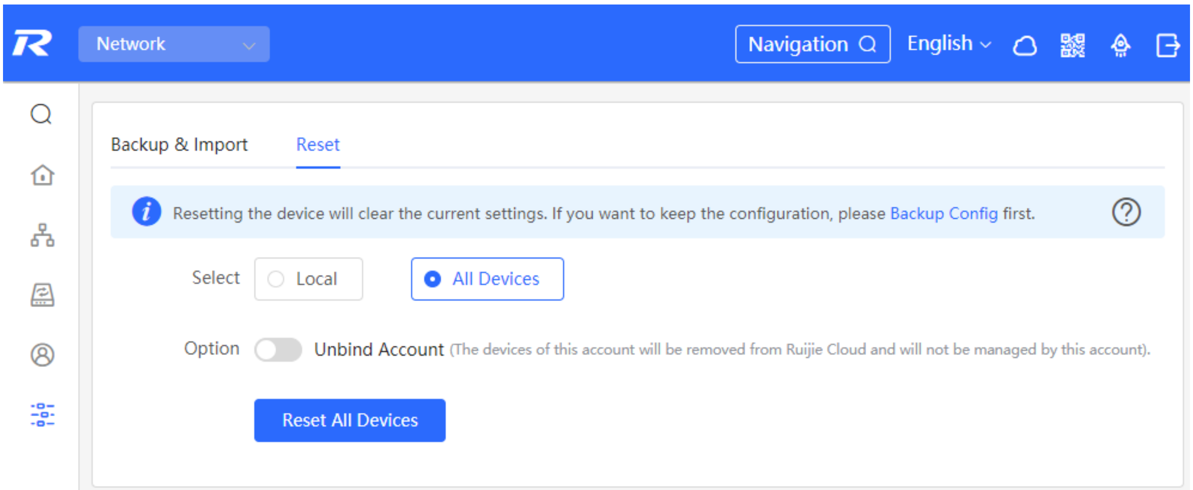
⚠ **Caution**

Resetting the device will clear current settings and reboot the device. If a useful configuration exists in the current system, you can export the current configuration (see 10.4) before restoring the factory settings. Exercise caution when performing this operation.

18.5.2 Resetting the Devices in the Network

Choose **Network** > **System** > **Management** > **Reset**.

Select **All Devices** and choose whether to **Unbind Account**, click **Reset All Devices** and all devices in the current network will be restored to their factory settings.



Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.

Select ○ Local ● All Devices

Option Unbind Account (The devices of this account will be removed from Ruijie Cloud and will not be managed by this account).

Caution

Resetting the network will clear current settings of all devices in the network and reboot the devices. Exercise caution when performing this operation.

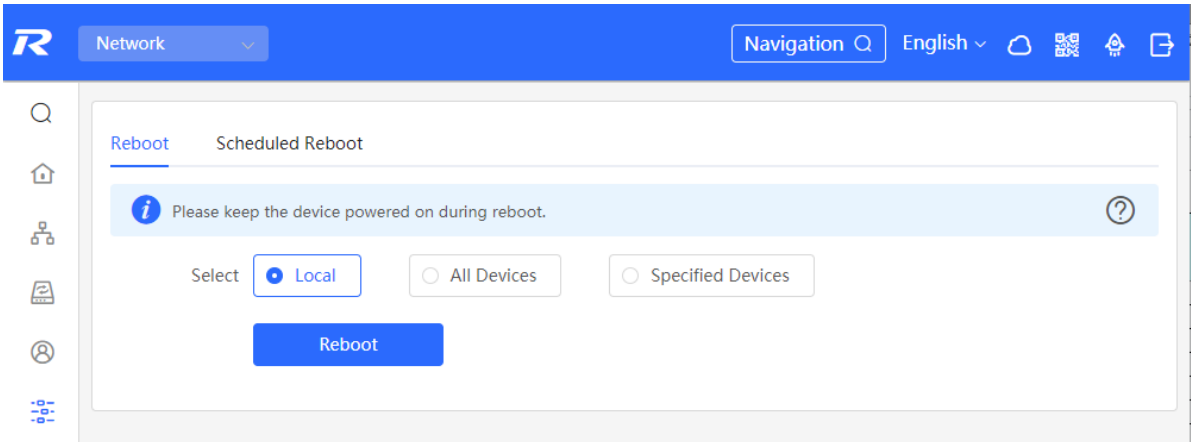
18.6 Rebooting the Device

18.6.1 Rebooting the Device

Choose **Self-Organizing Mode** > **Network** > **System** > **Management** > **Reset**.

Choose **Standalone Mode** > **System** > **Reboot**.

Select **Local** and click **All Devices**. The device will restart. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.



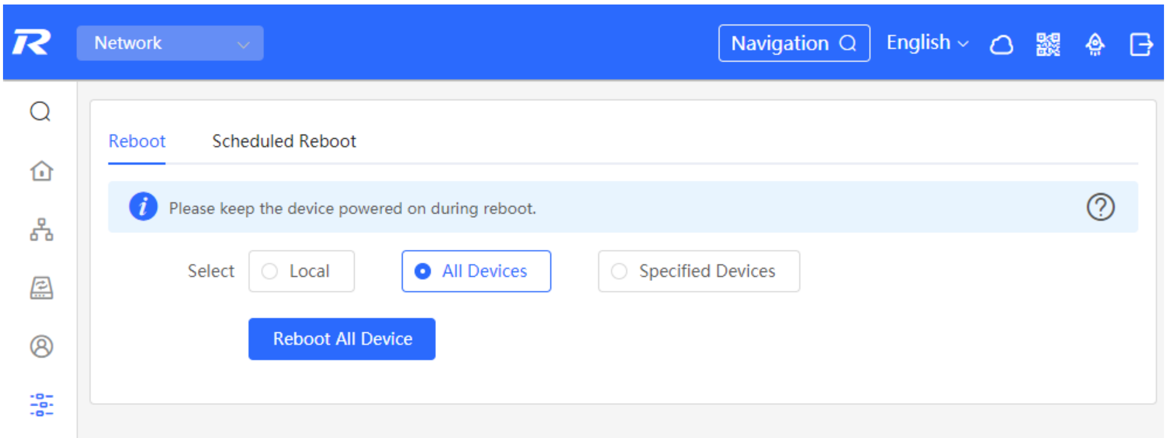
Please keep the device powered on during reboot.

Select ● Local ○ All Devices ○ Specified Devices

18.6.2 Rebooting the Devices in the Network

Choose **Network** > **System** > **Reboot** > **Reboot**.

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.



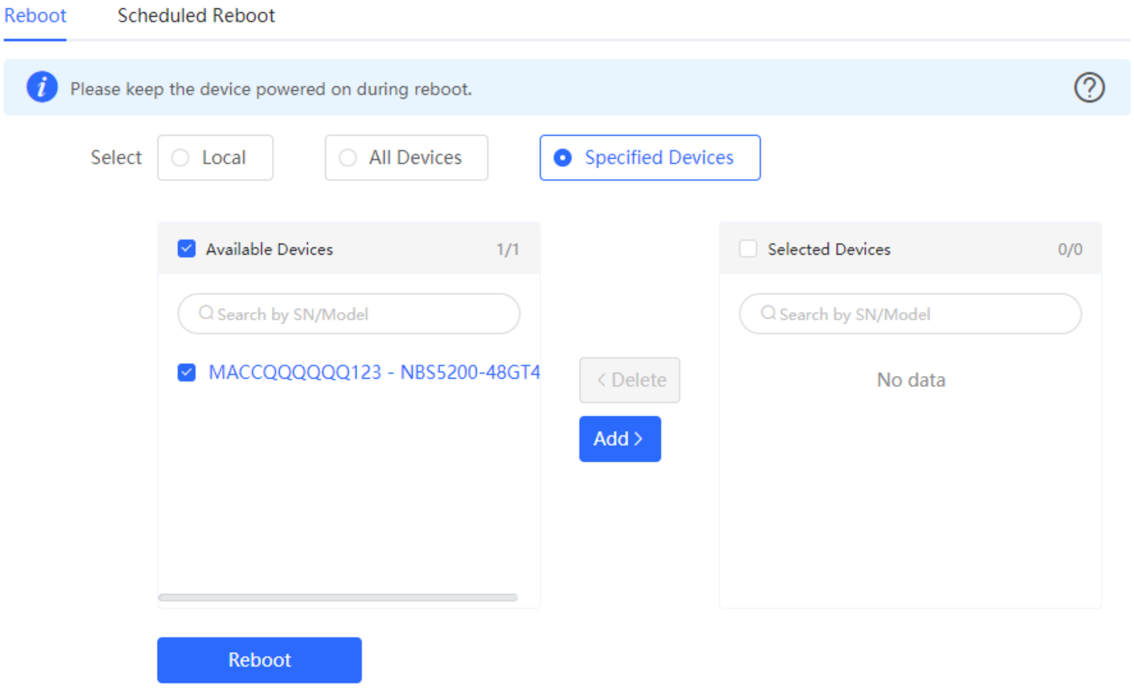
Caution

It will take some time for the network to reboot, please be patient. The network operation will affect the entire network. Therefore, exercise caution when performing this operation.

18.6.3 Rebooting Specified Devices in the Network

Choose **Network** > **System** > **Reboot** > **Reboot**.

Click **Specified Devices**, select desired devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.



18.7 Configuring Scheduled Reboot

Confirm that the system time is accurate. For details about how to configure the system time, see 18.1 . To avoid network interruption caused by device reboot at wrong time.

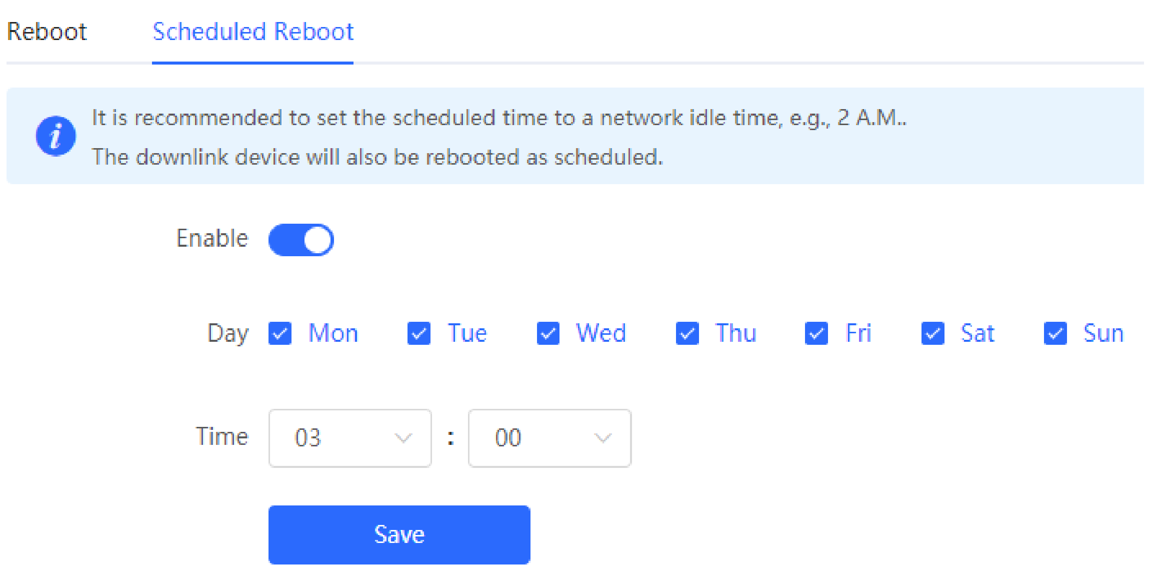
Choose **Self-Organizing Mode** > **Network** > **System**> **Scheduled Reboot**.

Choose **Standalone Mode** > **System** > **Scheduled Reboot**.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.

Caution

Once enable scheduled reboot in the network mode, all devices in the network will reboot when the system time matches to the timed time. Therefore, exercise caution when performing this operation.



It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable: on

Day ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time 03 : 00

18.8 Upgrade

Caution

- It is recommended to backup the configuration before software upgrade.
- Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

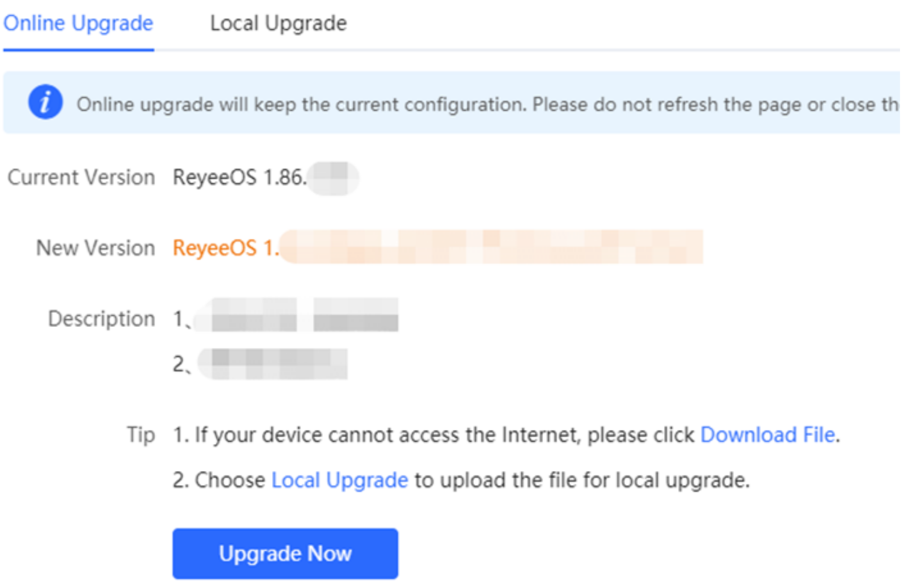
18.8.1 Online Upgrade

Choose **Local Device** > **System** > **Upgrade** > **Online Upgrade**.

The current page displays the current system version and allows you to detect whether a later version is available. If a new version is available, click **Upgrade Now** to perform online upgrade. If the network environment does not support online upgrade, click **Download File** to download the upgrade installation package locally and then perform local upgrade.

Note

- Online upgrade will retain the current configuration.
- Do not refresh the page or close the browser during the upgrade process. After successful upgrade, you will be redirected to the login page automatically.



Online Upgrade Local Upgrade

Online upgrade will keep the current configuration. Please do not refresh the page or close th

Current Version ReyeeOS 1.86.

New Version ReyeeOS 1.

Description 1、

2、

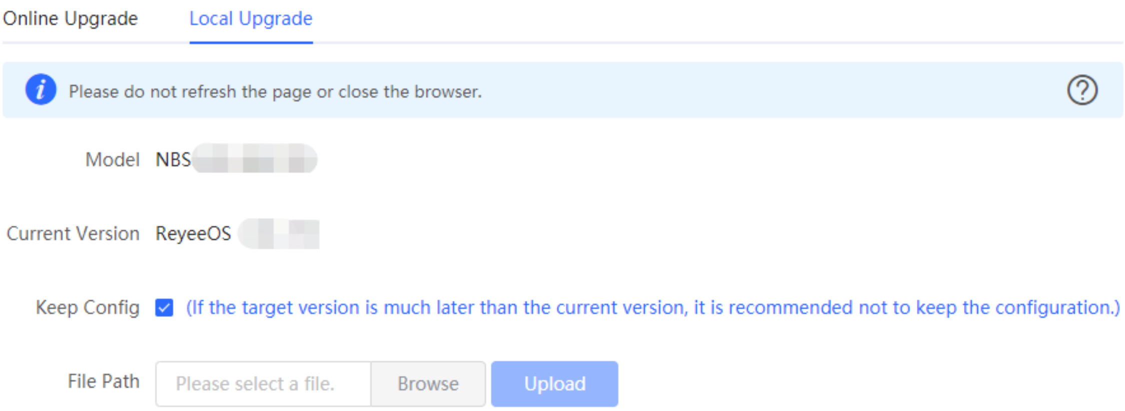
Tip 1. If your device cannot access the Internet, please click Download File.

2. Choose Local Upgrade to upload the file for local upgrade.

18.8.2 Local Upgrade

Choose **Local Device** > **System** > **Upgrade** > **Local Upgrade**.

Displays the device model and current software version. You can choose whether to keep the configuration upgrade or not. Click **Browse** to select the local software installation package, click **Upload** to upload the installation package and upgrade.



Online Upgrade Local Upgrade

Please do not refresh the page or close the browser.

Model NBS

Current Version ReyeeOS

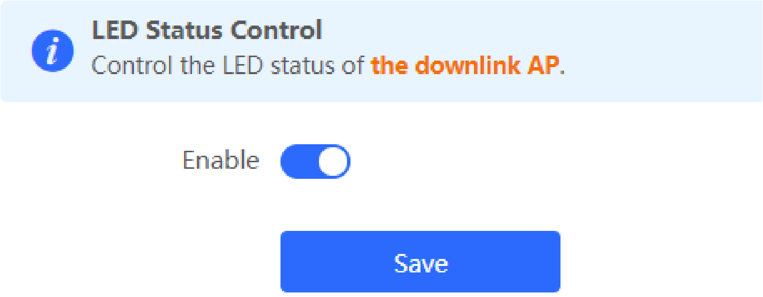
Keep Config ☑ (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path Please select a file.

18.9 LED

Choose **Network** > **Network** > **LED**.

Click the button to control the LED status of the downlink AP. Click **Save** to deliver the configuration and make it take effect.



LED Status Control

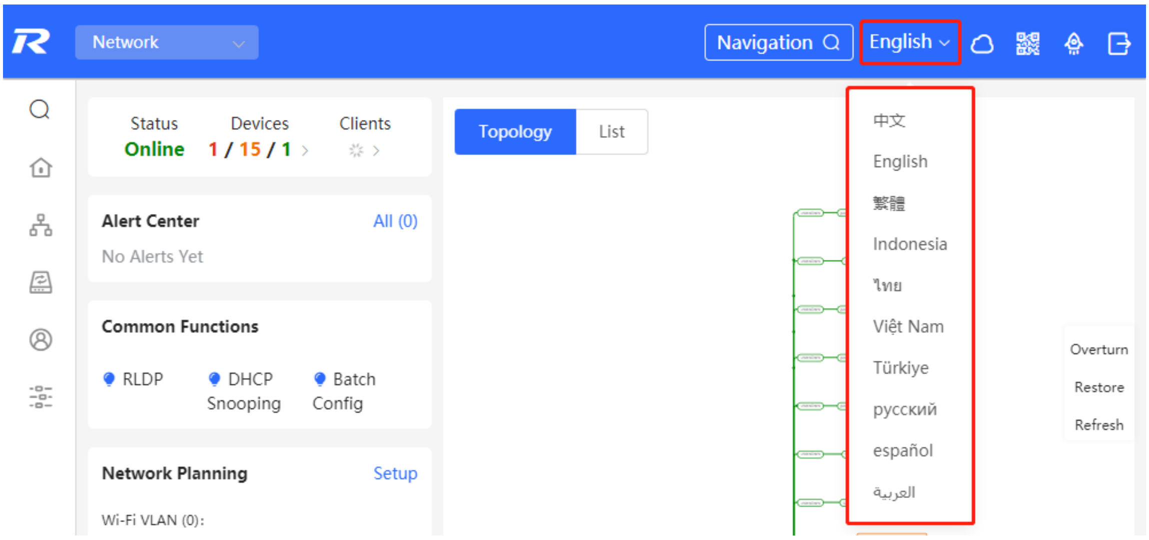
Control the LED status of **the downlink AP**.

Enable ●

18.10 Switching the System Language

Click English ⌄ in the upper-right corner of the Web page.

Click a required language to switch the system language.



19 NBS Series Wi-Fi Network Setup

Note

- To manage other devices in the self-organizing network, enable the self-organizing network discovery function. (See Switching the Work Mode)The wireless settings are synchronized to all wireless devices in the network by default. You can configure groups to limit the device scope under wireless management. For details, see 19.1 .
- The device itself does not support transmitting wireless Wi-Fi signals, and the wireless settings need to be synchronized to the wireless devices in the network to take effect.

19.1 Configuring AP Groups

19.1.1 Overview

After self-organizing network discovery is enabled, the device can function as the master AP/AC to batch configure and manage its downlink APs by group. Before you configure the APs, divide them to different groups.

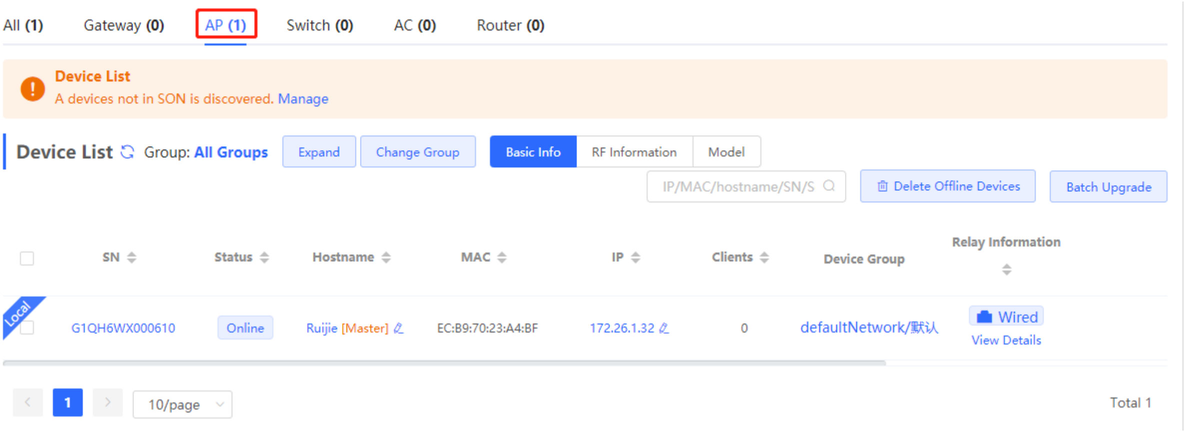
Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

19.1.2 Procedure

Choose **Network** > **Devices** > **AP**.

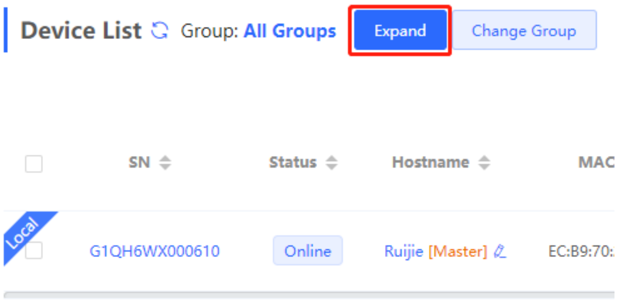
(1) View the information of all APs in the current network, including the basic information, RF information, and model. Click the SN of an AP to configure the AP separately.



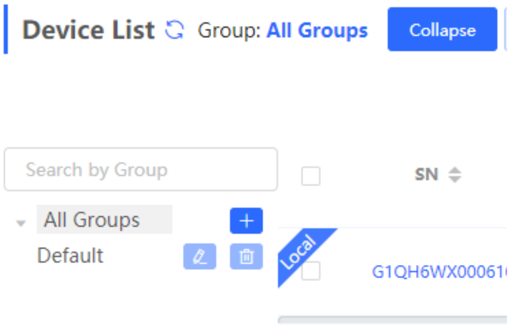
Device List
A devices not in SON is discovered. Manage

	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
□	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	defaultNetwork/默认	Wired View Details

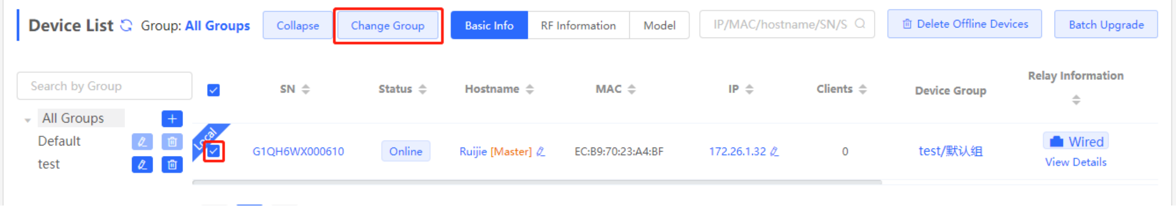
(2) Click **Expand**. Information of all the current groups is displayed to the left of the list. Click + to create a group. You can create a maximum of eight groups. Select the target group and click ✎ to modify the group name or click 🗑 to delete the group. You cannot modify the name of the default group or delete the default group.



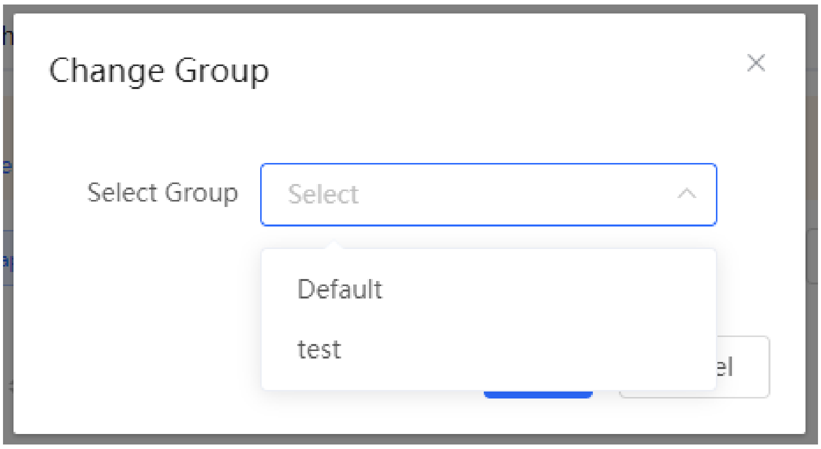
□	SN	Status	Hostname	MAC
□	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:



(3) Click a group name in the left. All APs in the group are displayed. One AP can belong to only one group. By default, all APs belong to the default group. Select a record in the device list and click **Change Group** to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click **Delete Offline Devices** to remove offline devices from the list.



☑	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
☑	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	test/默认组	Wired View Details



19.2 Configuring Wi-Fi

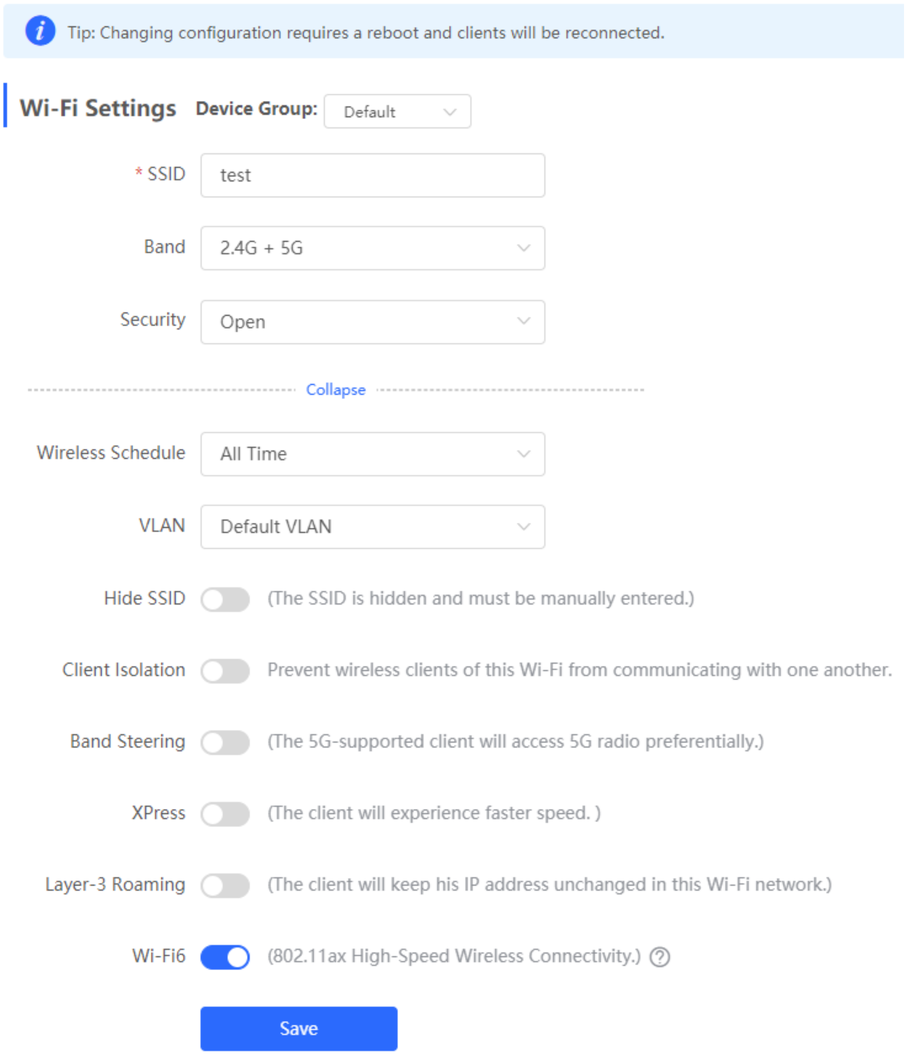
Choose **Network** > **Wi-Fi** > **Wi-Fi Settings**.

Enter the Wi-Fi name and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click **Save**.

Click **Advanced Settings** to configure more Wi-Fi parameters.

⚠ **Caution**

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: test

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID ○ (The SSID is hidden and must be manually entered.)

Client Isolation ○ Prevent wireless clients of this Wi-Fi from communicating with one another.

Band Steering ○ (The 5G-supported client will access 5G radio preferentially.)

XPress ○ (The client will experience faster speed.)

Layer-3 Roaming ○ (The client will keep his IP address unchanged in this Wi-Fi network.)

Wi-Fi6 ● (802.11ax High-Speed Wireless Connectivity.) ⓘ

Table 11-1 Wireless Network Configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is 2.4G + 5G, indicating that the device provides signals at both 2.4 GHz

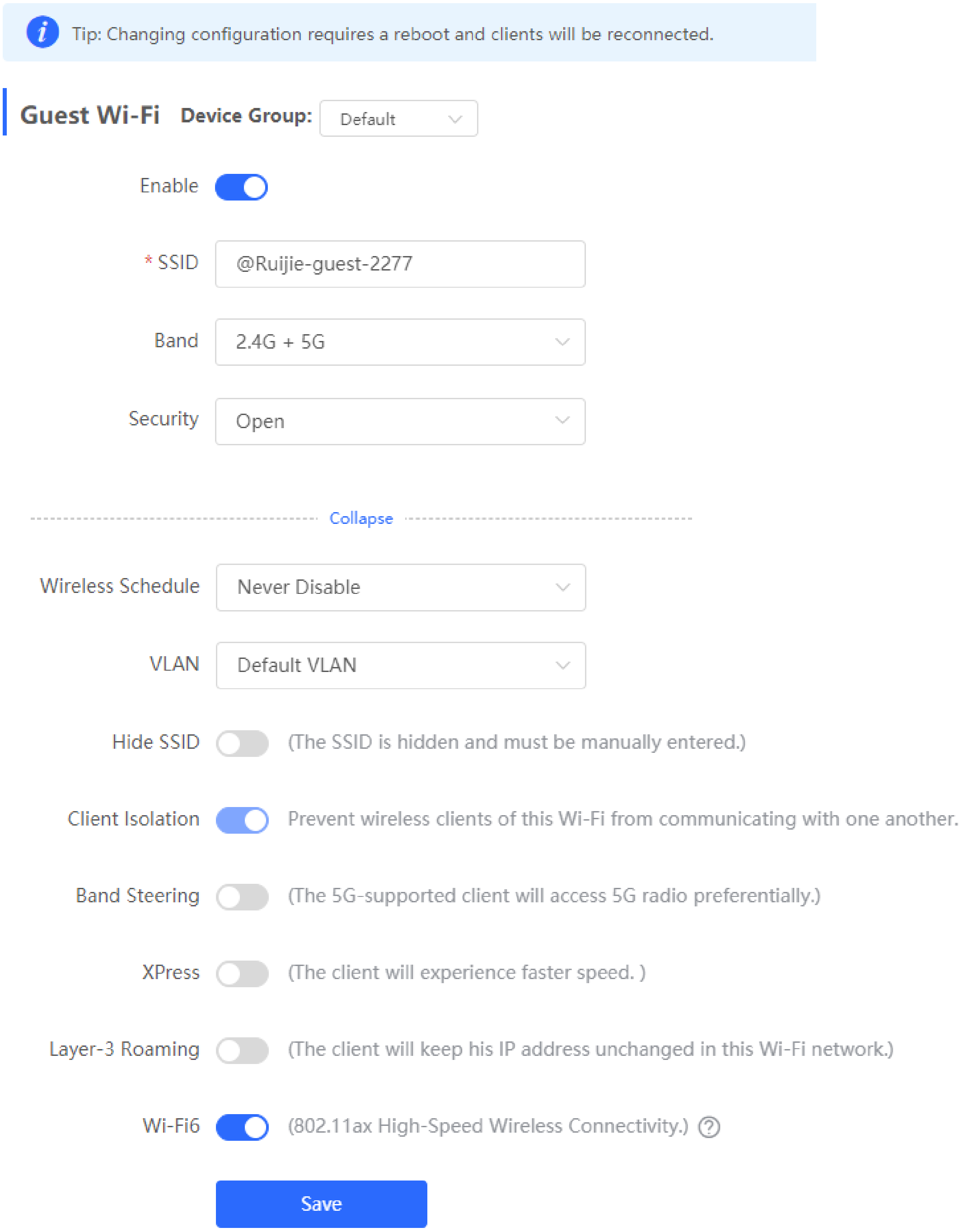
Parameter	Description
	and 5 GHz bands.
Security	Select an encryption mode for the wireless network connection. The options are as follows: Open: The device can associate with Wi-Fi without a password. WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for encryption.
Wi-Fi Password	Specify the password for connection to the wireless network. The password is a string of 8 to 16 characters.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the Wi-Fi name after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current Wi-Fi name before you enable this function.
Client Isolation	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G.
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
Wi-Fi6	After this function is enabled, wireless users can have faster network access speed and optimized network access experience. This function is valid only on APs and routers supporting 802.11ax. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function.

19.3 Configuring Guest Wi-Fi

Choose **Network** > **Wi-Fi** > **Guest Wi-Fi**.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. **Client Isolation** is enabled for guest Wi-Fi by default, and it cannot be disabled. In this case, users associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Turn on the guest Wi-Fi and set the guest Wi-Fi name and password. Click **Expand** to configure the wireless schedule of the guest Wi-Fi and more Wi-Fi parameters. (For details, see 19.2 .) Click **Save**. Guests can access the Internet through Wi-Fi after entering the Wi-Fi name and password.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable

* SSID: @Ruijie-guest-2277

Band: 2.4G + 5G

Security: Open

Collapse

Wireless Schedule: Never Disable

VLAN: Default VLAN

Hide SSID (The SSID is hidden and must be manually entered.)

Client Isolation Prevent wireless clients of this Wi-Fi from communicating with one another.

Band Steering (The 5G-supported client will access 5G radio preferentially.)

XPress (The client will experience faster speed.)

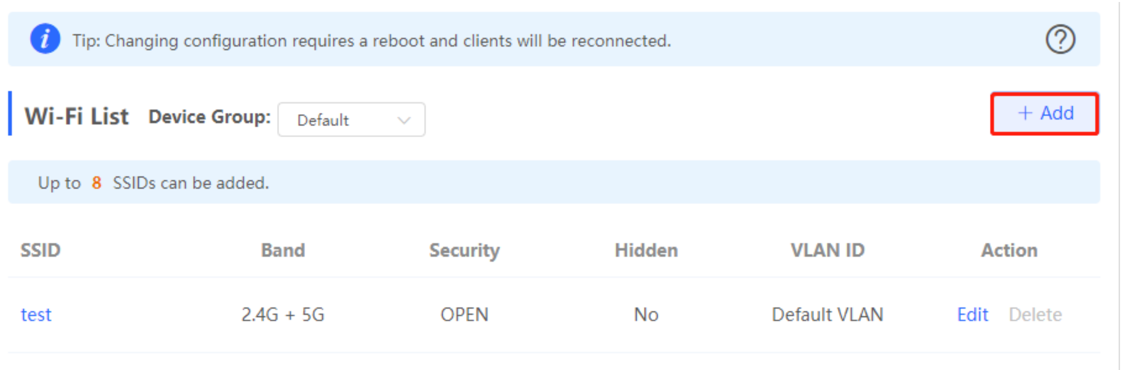
Layer-3 Roaming (The client will keep his IP address unchanged in this Wi-Fi network.)

Wi-Fi6 (802.11ax High-Speed Wireless Connectivity.)

19.4 Adding a Wi-Fi

Choose **Network** > **Wi-Fi** > **Wi-Fi List**.

Click **Add**, enter the Wi-Fi name and password, and click **OK** to create a Wi-Fi. Click **Expand** to configure more Wi-Fi parameters. For details, see 19.2 . After a Wi-Fi is added, clients can find this Wi-Fi, and the Wi-Fi information is displayed in the Wi-Fi list.

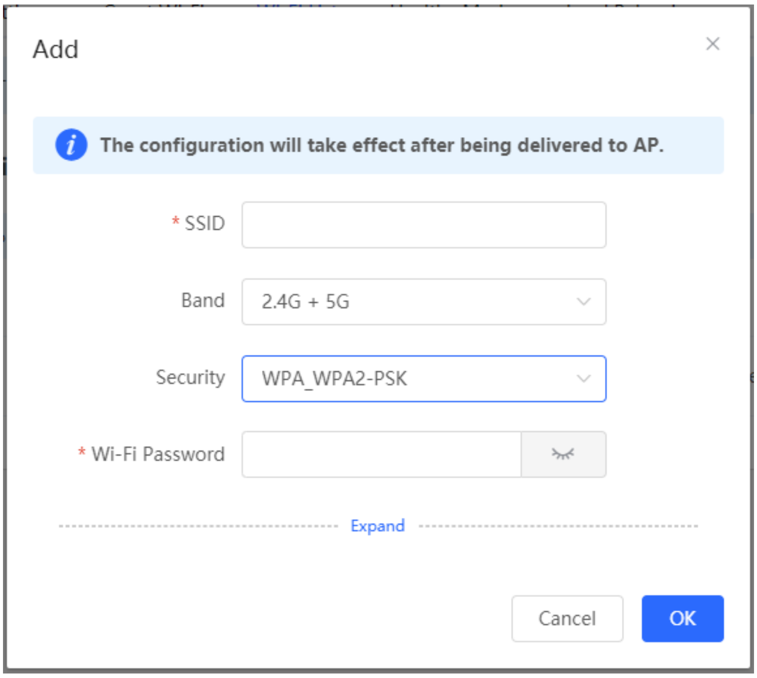


Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
test	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete



Add

The configuration will take effect after being delivered to AP.

* SSID

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

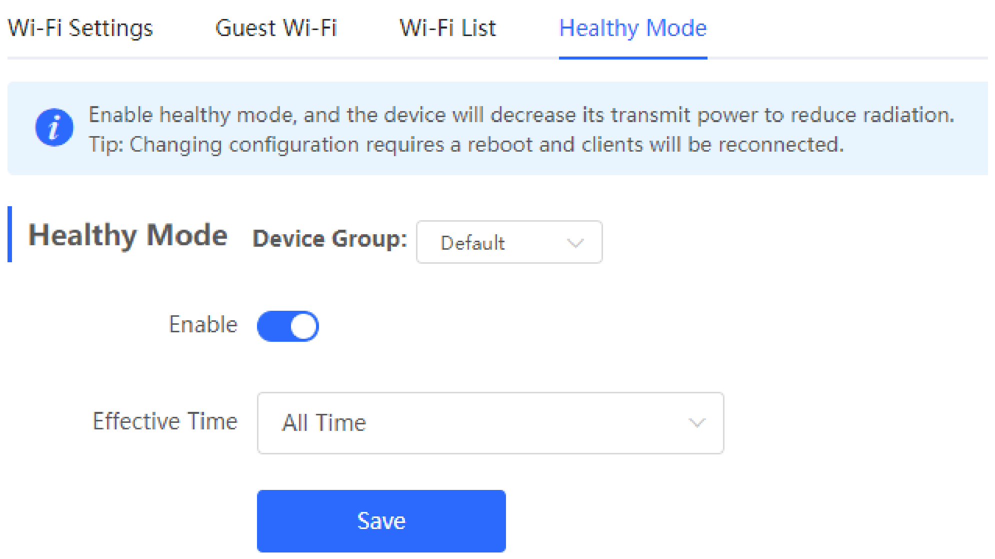
* Wi-Fi Password

19.5 Healthy Mode

Choose **Network** > **Wi-Fi** > **Healthy Mode**.

Turn on healthy mode and select a wireless schedule for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the wireless device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable healthy mode or set the wireless schedule to the idle periods.



Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.

Healthy Mode Device Group: Default

Enable: on

Effective Time: All Time

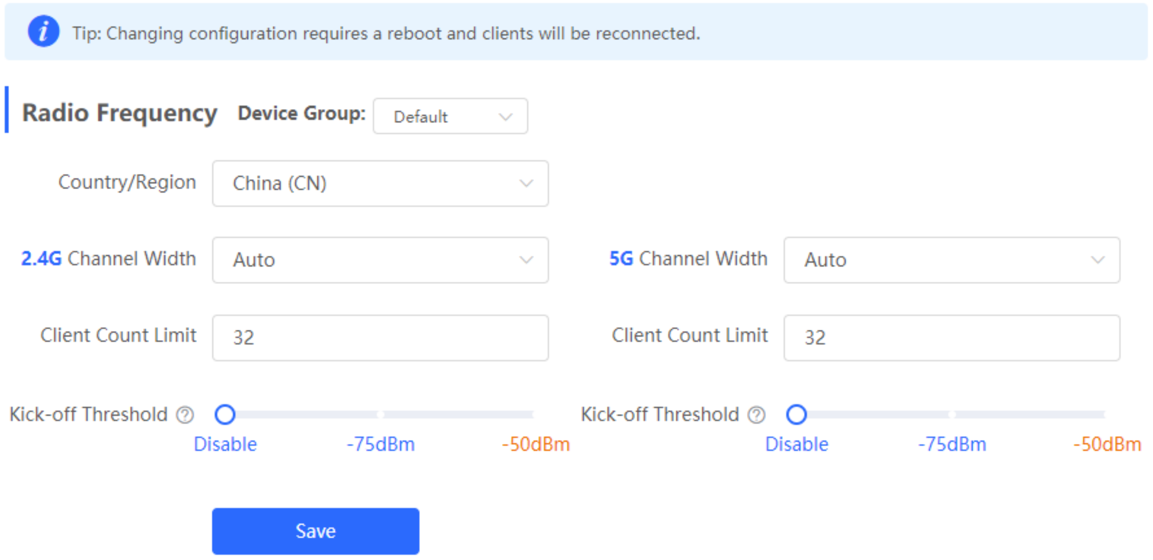
19.6 RF Settings

Choose **Network** > **Network** > **Radio Frequency**.

The wireless device can detect the surrounding wireless environment upon power-on and select properconfiguration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit: 32

Client Count Limit: 32

Kick-off Threshold: Disable

Kick-off Threshold: Disable

Table 11-2 RF Configuration

Parameter	Description
Country/Region	The Wi-Fi channels stipulated by each country may be different. To ensure that clients can find the Wi-Fi signal, select the country or region where the device is located.
2.4G/5G Channel Width	A lower bandwidth indicates more stable network, and a higher bandwidth indicates easier interference. In case of severe interference, select a relatively low bandwidth to prevent network freezing to certain extent. The 2.4 GHz band supports the 20 MHz and 40 MHz bandwidths. The 5 GHz band supports the 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is Auto, indicating that the bandwidth is selected automatically based on the environment.
Client Count Limit	If a large number of users access the AP or router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. After you set this parameter, new user access is prohibited when the number of access users reaches the specified value. If the clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Kick-off Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality to some extent. When a client is far away from the wireless device, the Wi-Fi connection is disconnected when the wireless signal strength of the end user is lower than the kick-off threshold. In this case, the client has to select a nearer wireless signal. The client is prone to be kicked off if the kick-off threshold is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to Disable or a value smaller than -75 dBm.

Note

- Wireless channels available for your selection are determined by the country code. Select the country code based on the country or region of your device.
- Channel, transmit power, and roaming sensitivity cannot be set globally, and the devices should be configured separately.

19.7 Configuring Wi-Fi Blacklist or Whitelist

19.7.1 Overview

You can configure the global or SSID-based blacklist and whitelist. The MAC address supports full match and OUI match.

Wi-Fi blacklist: Clients in the Wi-Fi blacklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blacklist are free to access the Internet.

Wi-Fi whitelist: Only clients in the Wi-Fi whitelist can access the Internet. Clients that are not added to the Wi-Fi whitelist are prevented from accessing the Internet.

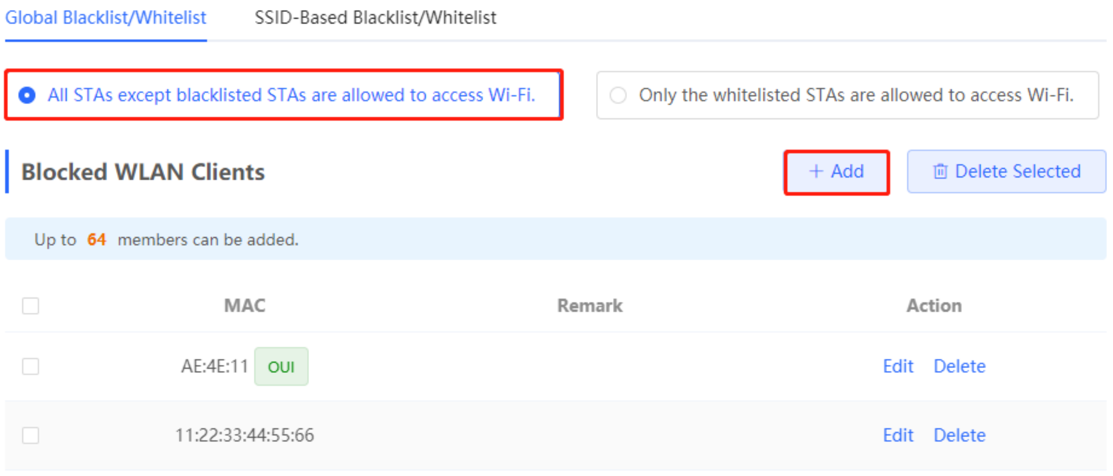
⚠ **Caution**

If the whitelist is empty, the whitelist does not take effect. In this case, all clients are allowed to access the Internet.

19.7.2 Configuring a Global Blacklist/Whitelist

Choose **Clients** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist client. In the **Add** window, enter the MAC address and remark of the target client and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the access point.



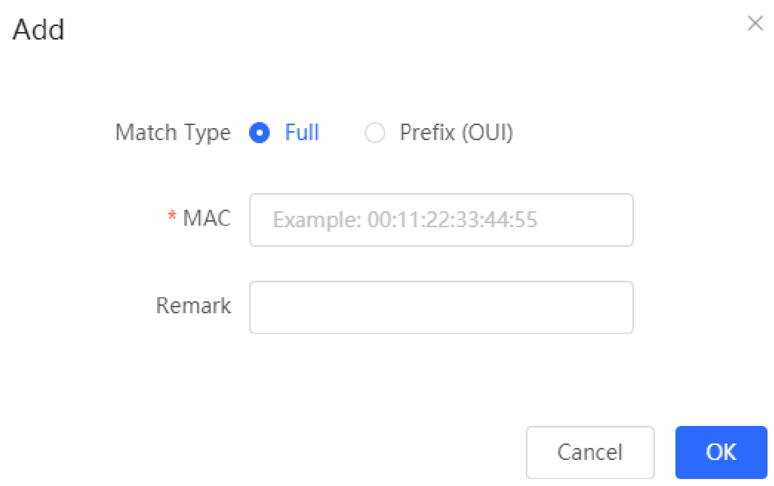
● All STAs except blacklisted STAs are allowed to access Wi-Fi.

○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 64 members can be added.

□	MAC	Remark	Action
□	AE:4E:11 OUI		Edit Delete
□	11:22:33:44:55:66		Edit Delete



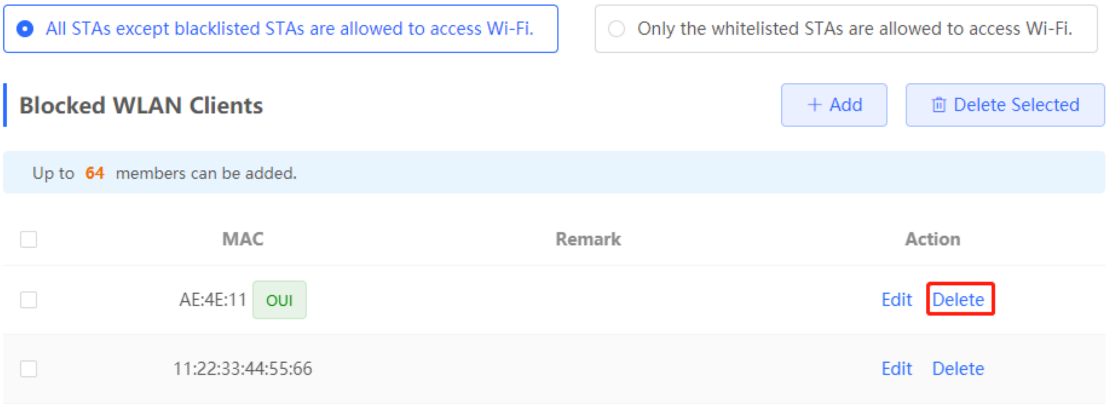
Add ×

Match Type ● Full ○ Prefix (OUI)

* MAC Example: 00:11:22:33:44:55

Remark

If you click **Delete** in black list mode, the corresponding client can reconnect to Wi-Fi; if you click **Delete** in whitelist mode and the whitelist list is not empty after deletion, the corresponding client will be disconnected and prohibited from connecting to Wi-Fi.



● All STAs except blacklisted STAs are allowed to access Wi-Fi.   ○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

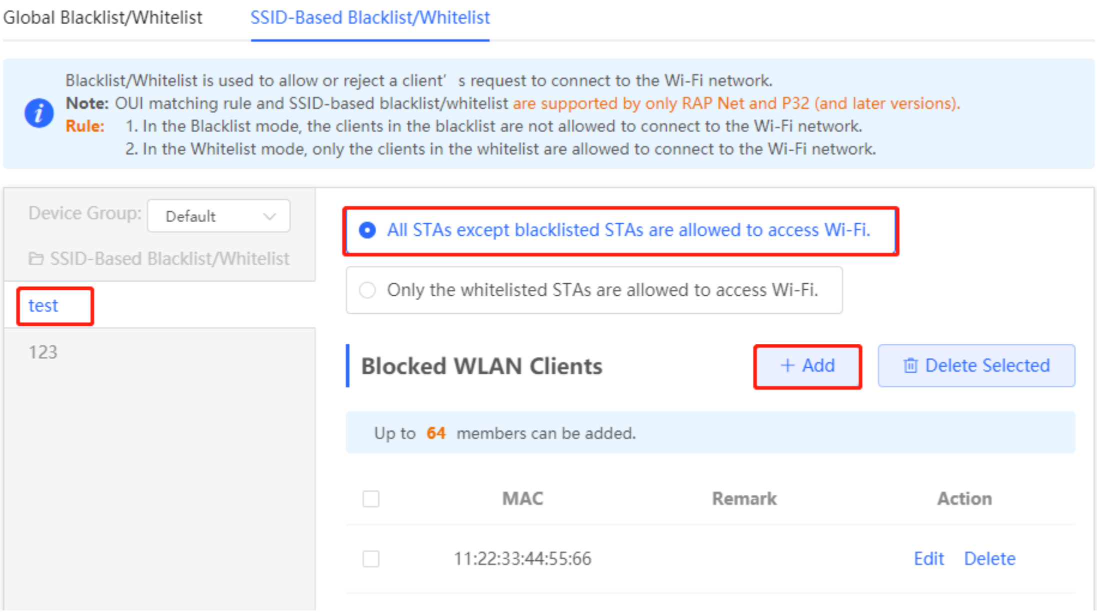
Up to 64 members can be added.

□	MAC	Remark	Action
□	AE:4E:11 OUI		Edit Delete
□	11:22:33:44:55:66		Edit Delete

19.7.3 Configuring an SSID-based Blacklist/Whitelist

Choose **Clients** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

Select a target Wi-Fi network from the left column, select the blacklist or whitelist mode, and click **Add** to configure a blacklist or whitelist client. The SSID-based blacklist and whitelist will restrict the client access to the specified Wi-Fi.



Blacklist/Whitelist is used to allow or reject a client' s request to connect to the Wi-Fi network.
Note: OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).
Rule: 1. In the Blacklist mode, the clients in the blacklist are not allowed to connect to the Wi-Fi network.
2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the Wi-Fi network.

Device Group: Default

● All STAs except blacklisted STAs are allowed to access Wi-Fi.
○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 64 members can be added.

□	MAC	Remark	Action
□	11:22:33:44:55:66		Edit Delete

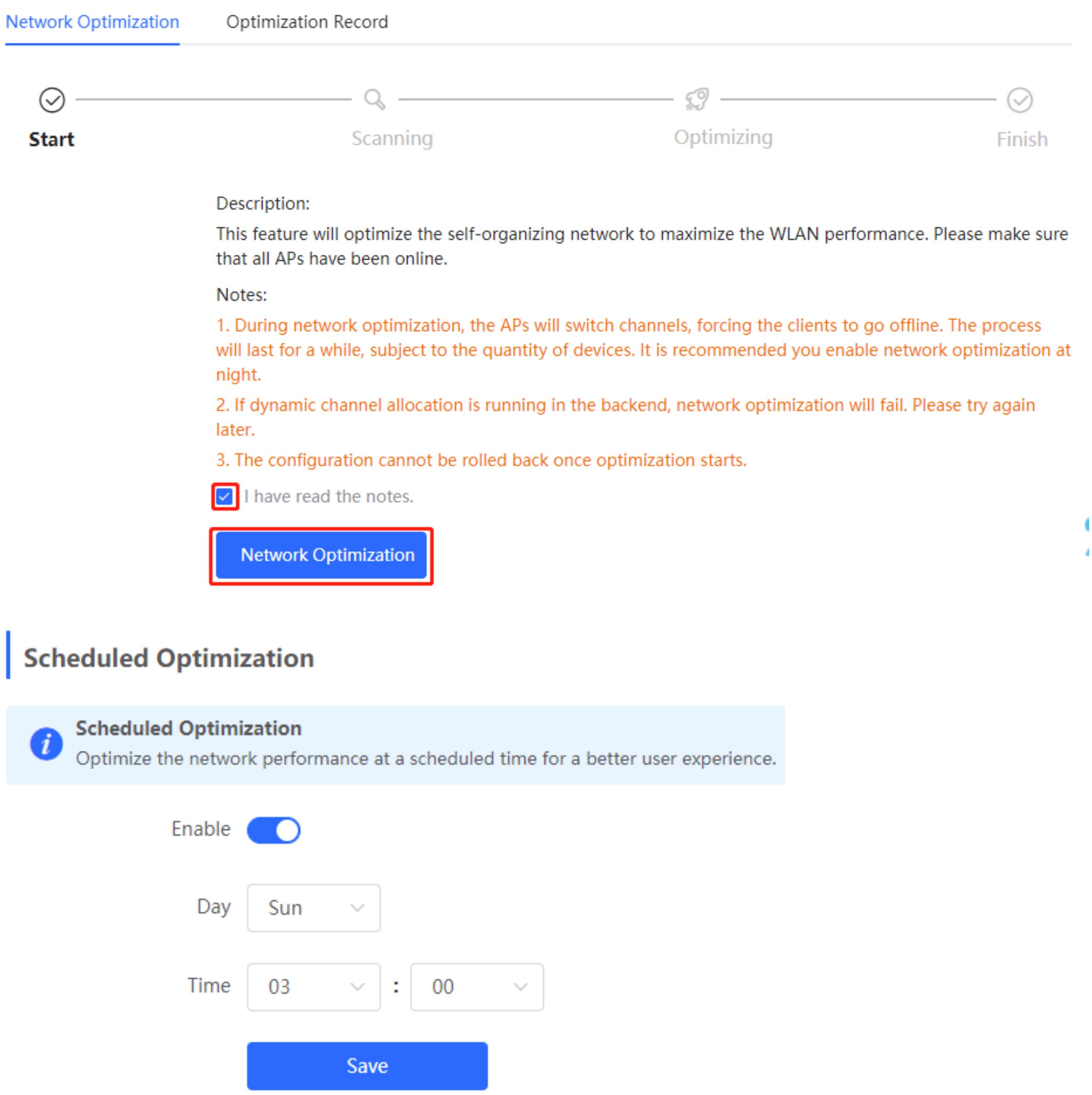
19.8 Wireless Network Optimization with One Click

Choose **Network** > **WIO**.

On the **Network Optimization** tab, select **I have read the notes** and click **Network Optimization** to perform automatic wireless network optimization in the networking environment. You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

Caution

Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.



Description:

This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.

Notes:

1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.

2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.

3. The configuration cannot be rolled back once optimization starts.

☑ I have read the notes.

Scheduled Optimization

Scheduled Optimization
Optimize the network performance at a scheduled time for a better user experience.

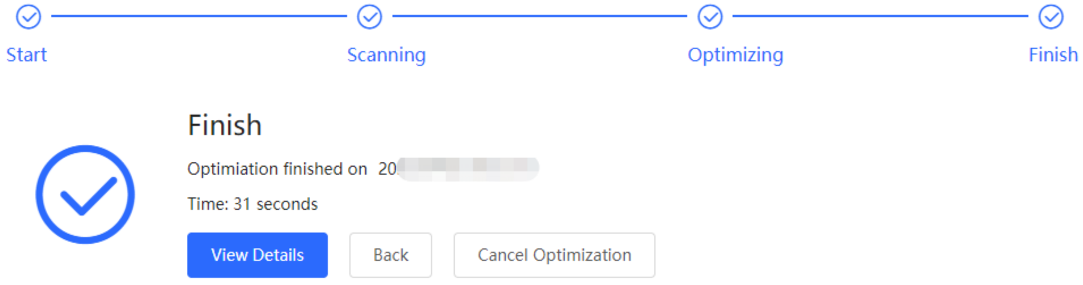
Enable: ●

Day: Sun

Time: 03 : 00

After optimization starts, please wait patiently until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.

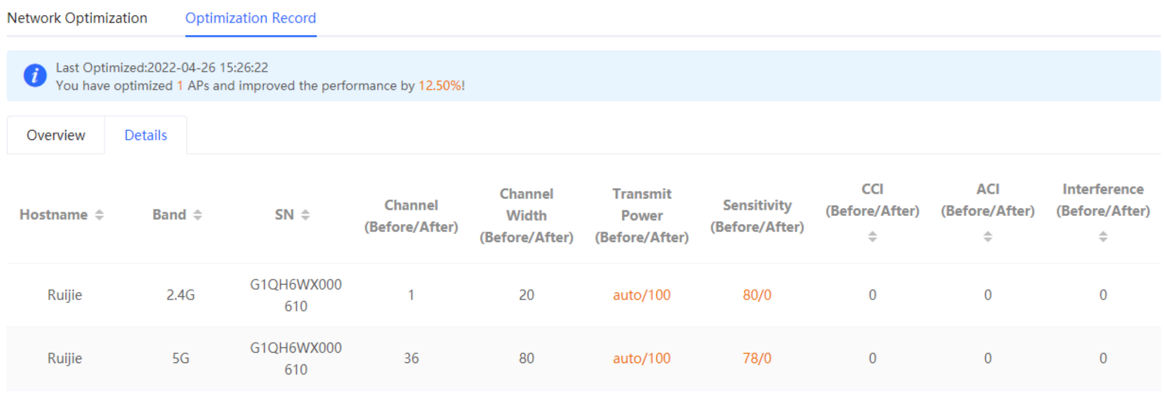
Click **View Details** or the **Optimization Record** tab to view the latest optimization record details.



Finish

Optimiation finished on 20[redacted]

Time: 31 seconds



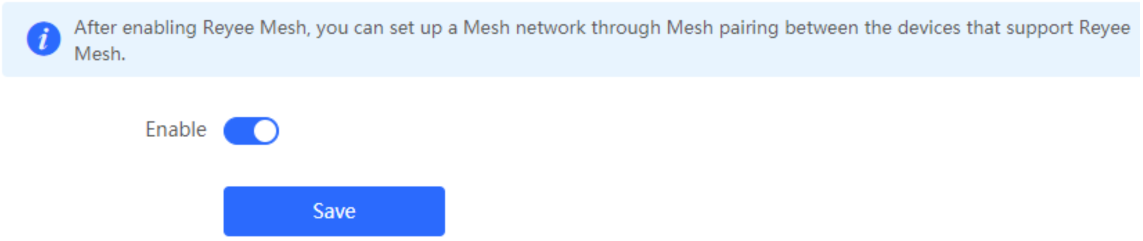
Last Optimized:2022-04-26 15:26:22
You have optimized 1 APs and improved the performance by 12.50%!

Hostname	Band	SN	Channel (Before/After)	Channel Width (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)	CCI (Before/After)	ACI (Before/After)	Interference (Before/After)
Ruijie	2.4G	G1QH6WX000610	1	20	auto/100	80/0	0	0	0
Ruijie	5G	G1QH6WX000610	36	80	auto/100	78/0	0	0	0

19.9 Enabling the Reyee Mesh Function

Choose **Network** > **Reyee Mesh**.

After the Reyee Mesh function is enabled, the devices that support EasyLink can be paired to form a mesh network. Devices can automatically search for new routers around them and pair with each other via the **Mesh** button, or log in to the router management page to search and select a new router for pairing.


After enabling Reyee Mesh, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh.

19.10 Configuring the AP Ports

Caution

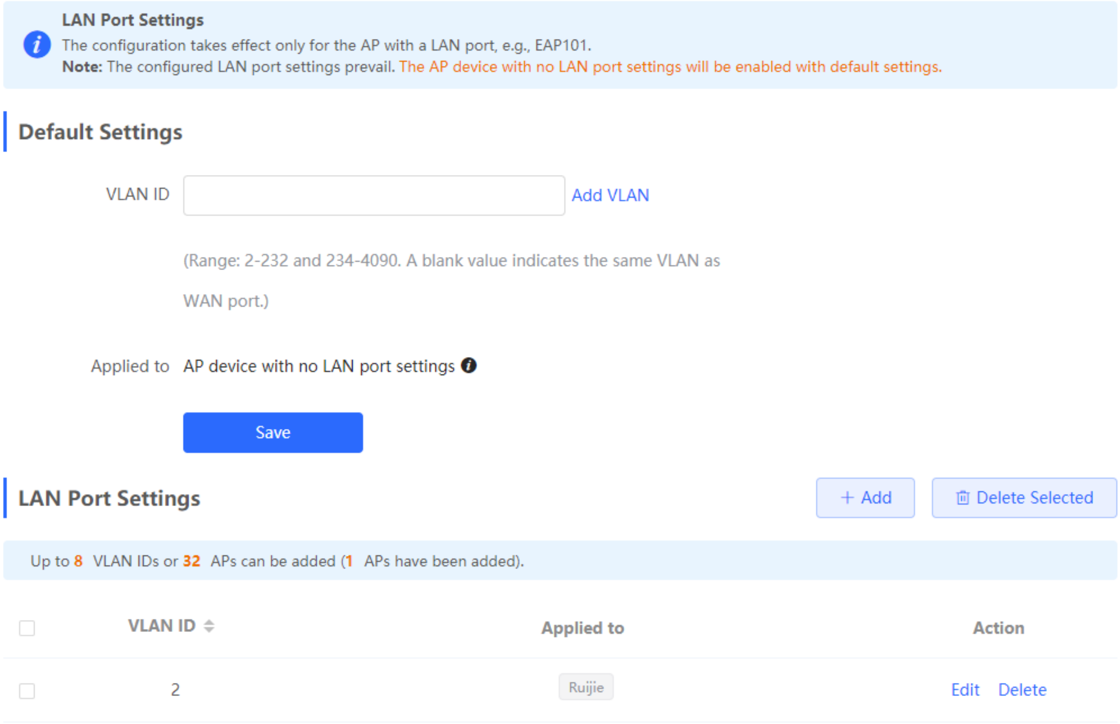
The configuration takes effect only on APs having wired LAN ports.

Choose **Network** > **LAN Ports**.

Choose **Network** > **LAN Ports**.

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.



LAN Port Settings
The configuration takes effect only for the AP with a LAN port, e.g., EAP101.
Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings.

Default Settings

VLAN ID: (blank) Add VLAN

(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.)

Applied to: AP device with no LAN port settings

Save

LAN Port Settings

+ Add | Delete Selected

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).

□	VLAN ID	Applied to	Action
□	2	Ruijie	Edit Delete

20 Advanced Solution Guide

20.1 Reyee Flow Control Solution

20.1.1 Application Scenario

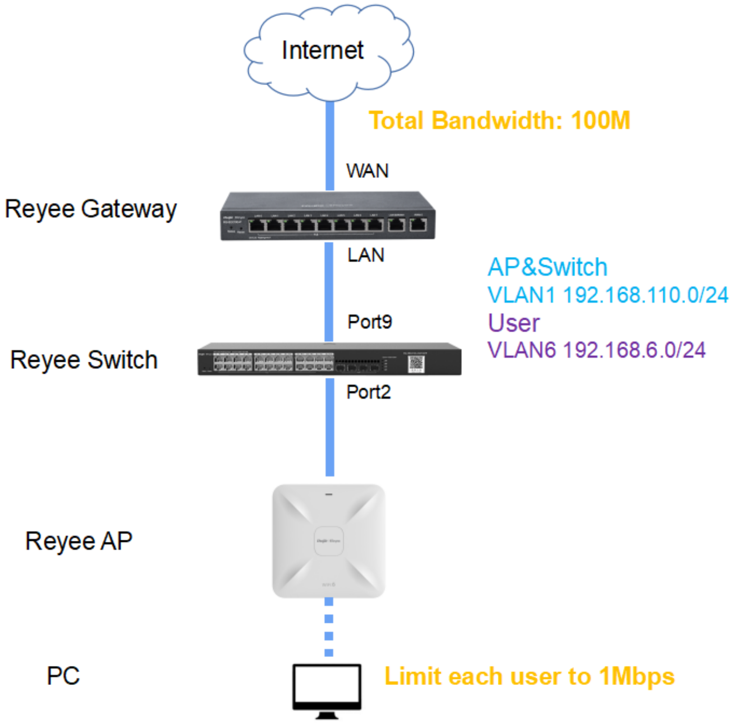
Flow Control is used for setting the rate limitations of download and upload for the clients. With the Flow Control configured, we can protect the network bandwidth from being occupied too much by some of the clients.

20.1.2 Configuration Case

Requirement

Limiting EG egress total bandwidth to 100Mbps and each user rate of VLAN 6 network segment to 1Mbps.

Network Topology



Network Description:

EG works as a DHCP server to assign IP addresses to users and AP & switch devices.

The AP & switch devices obtain the IP address 192.168.110.0/24 in the VLAN1 network segment for Internet access.

The users obtain the IP address 192.168.6.0/24 in the VLAN6 network segment for Internet access.

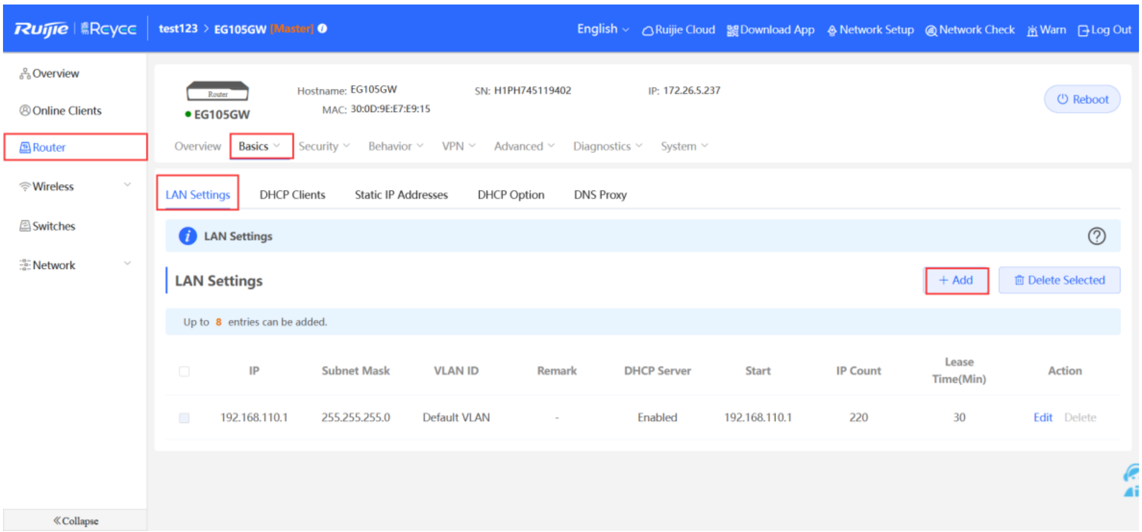
Configuration Steps

basic network configuration

Enable Smart Flow Control function and configure the custom policy

1. Configure basic network configuration

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN1 and VLAN6 network segment on the EG.

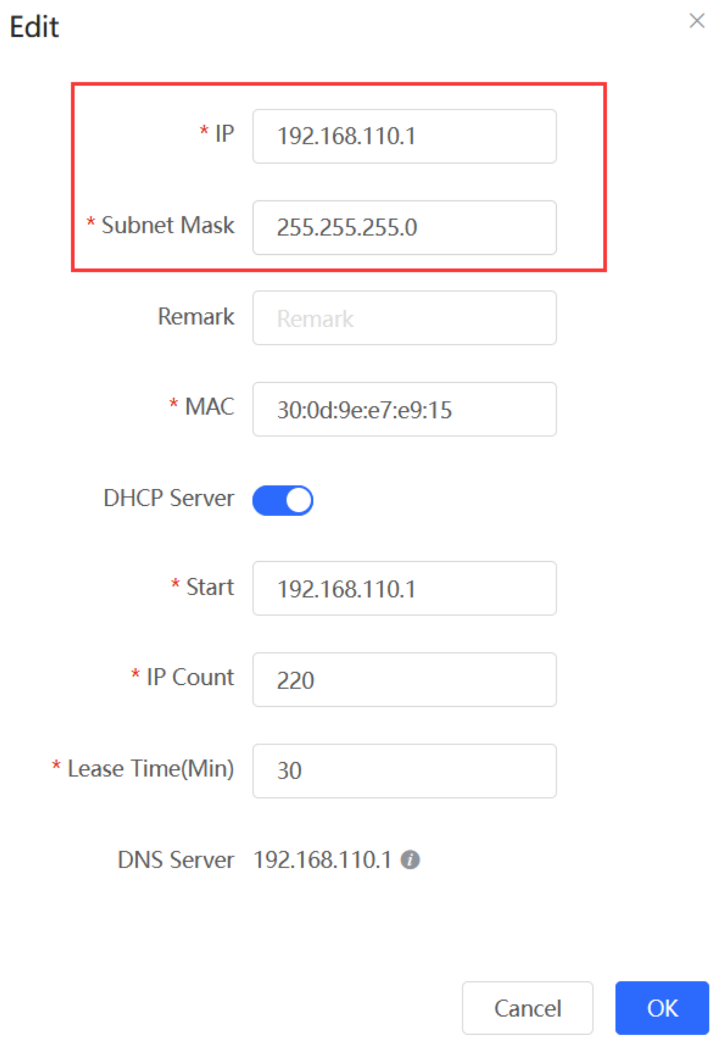


Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237

LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete



Edit

* IP: 192.168.110.1

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: 30:0d:9e:e7:e9:15

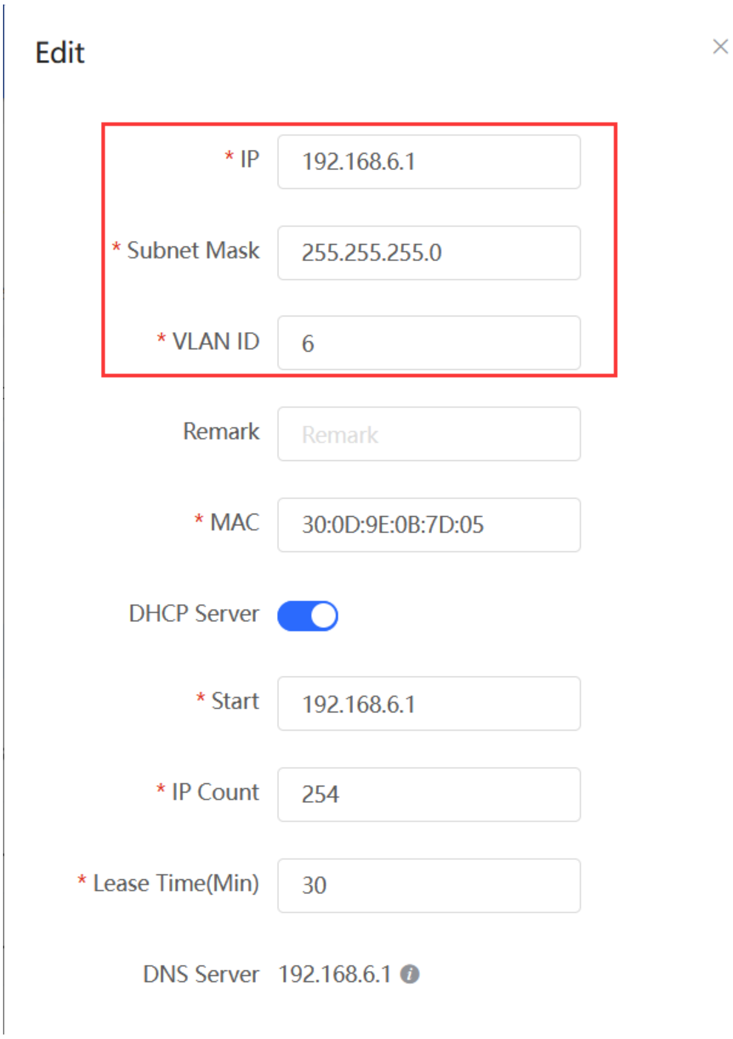
DHCP Server: ●

* Start: 192.168.110.1

* IP Count: 220

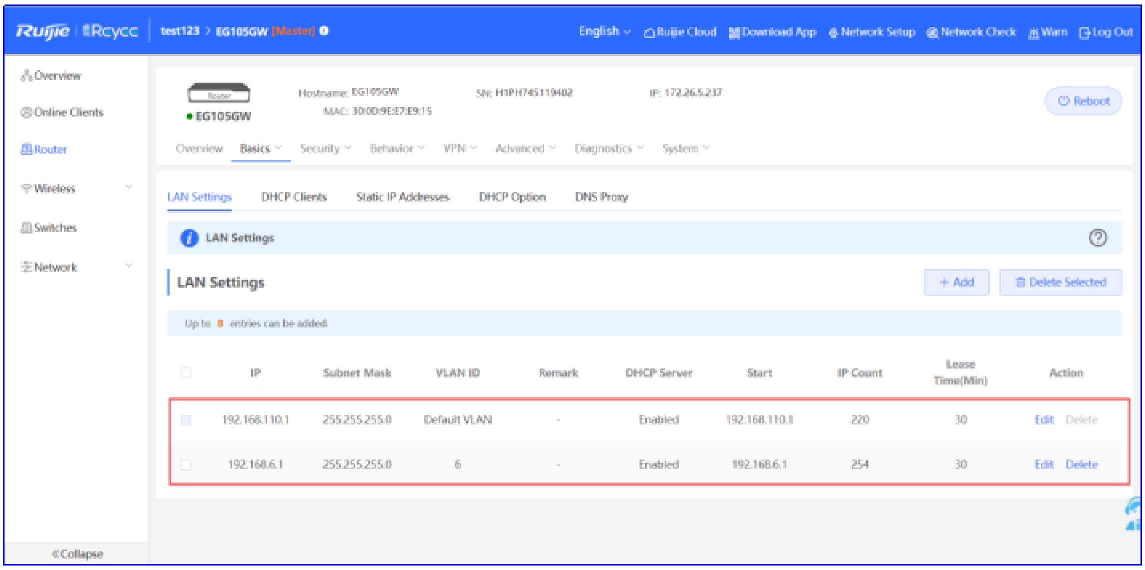
* Lease Time(Min): 30

DNS Server: 192.168.110.1



Edit

* IP	192.168.6.1
* Subnet Mask	255.255.255.0
* VLAN ID	6
Remark	Remark
* MAC	30:0D:9E:0B:7D:05
DHCP Server	●
* Start	192.168.6.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.6.1



EG105GW

Hostname: EG105GW SN: H1PH745119402 IP: 172.26.5.237

MAC: 30:0D:9E:E7:E9:15

LAN Settings

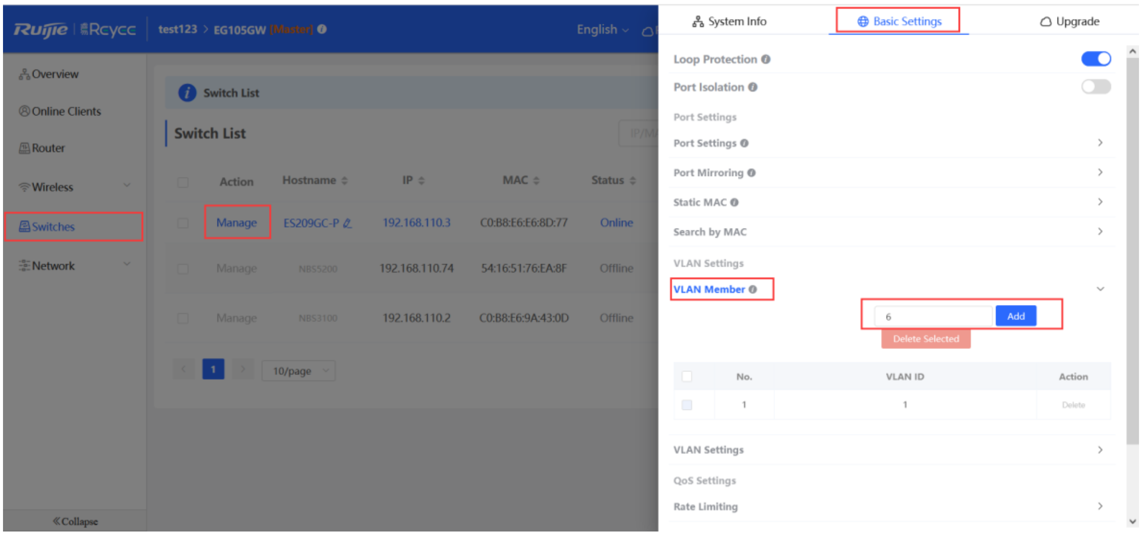
Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete

Note

Default VLAN 1 network is set to 192.168.110.0/24 network segment.

Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN6 on the switch, and click **VLAN Settings** to set port2 and port9 which connect to AP and EG to trunk port and allow the VLAN1 and VLAN6 to pass through, then check the port settings on the device.



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

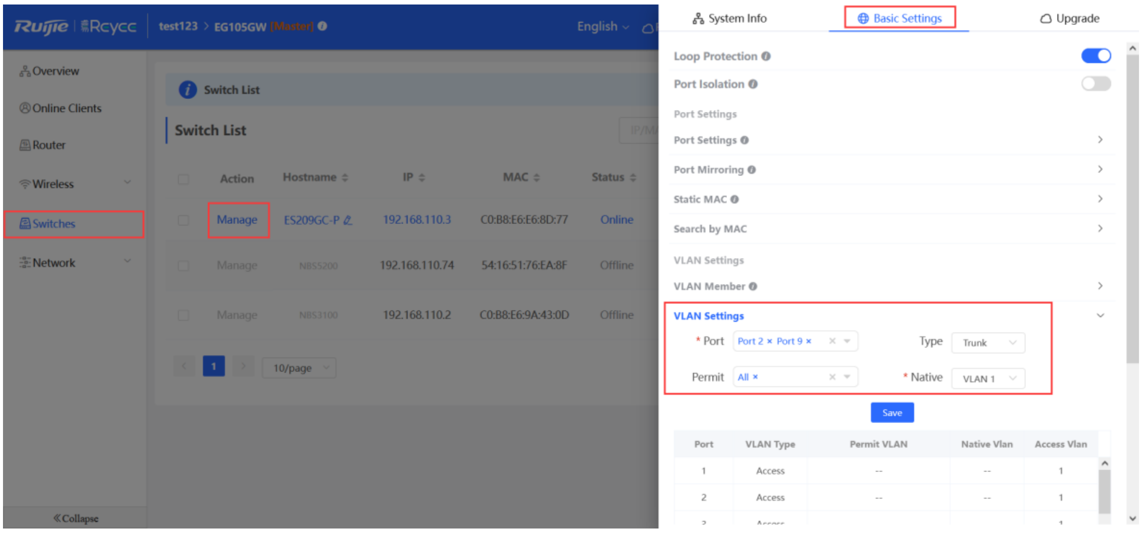
Loop Protection
Port Isolation

Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC

VLAN Settings
VLAN Member
6

No.	VLAN ID	Action
1	1	Delete

VLAN Settings
QoS Settings
Rate Limiting



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

Loop Protection
Port Isolation

Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC

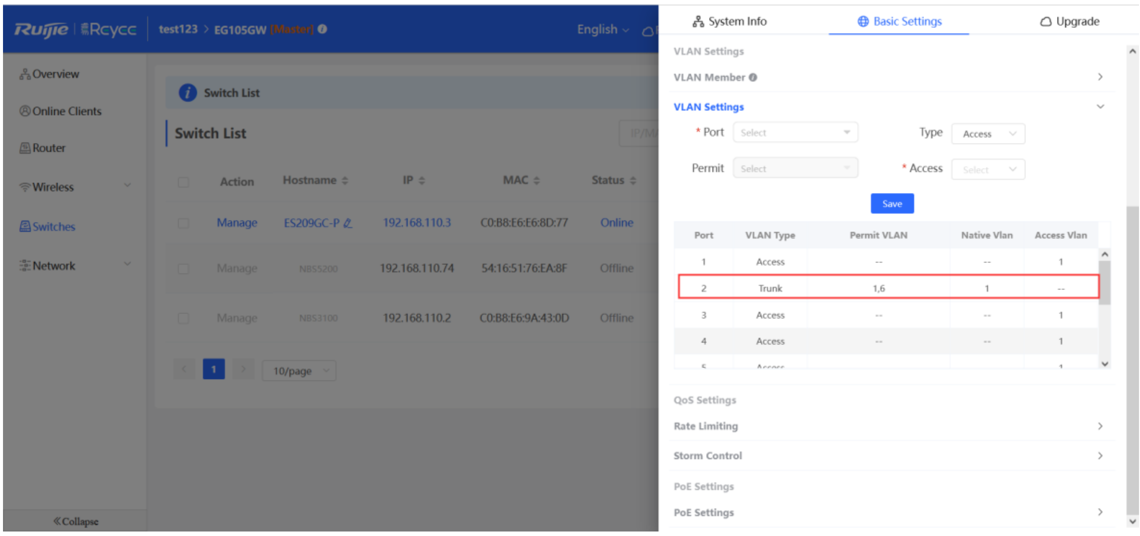
VLAN Settings
VLAN Member

VLAN Settings

* Port: Port 2 × Port 9 ×   Type: Trunk

Permit: All ×   * Native: VLAN 1

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Access	--	--	1



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

VLAN Settings
VLAN Member

VLAN Settings

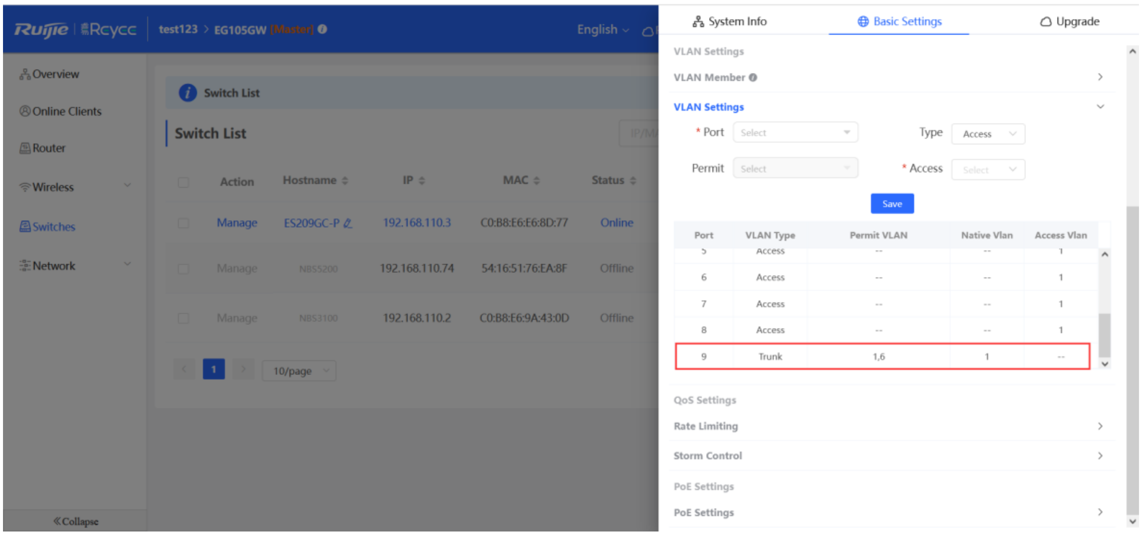
* Port: Select   Type: Access

Permit: Select   * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6	1	--
3	Access	--	--	1
4	Access	--	--	1

QoS Settings
Rate Limiting
Storm Control

PoE Settings
PoE Settings



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

10/page

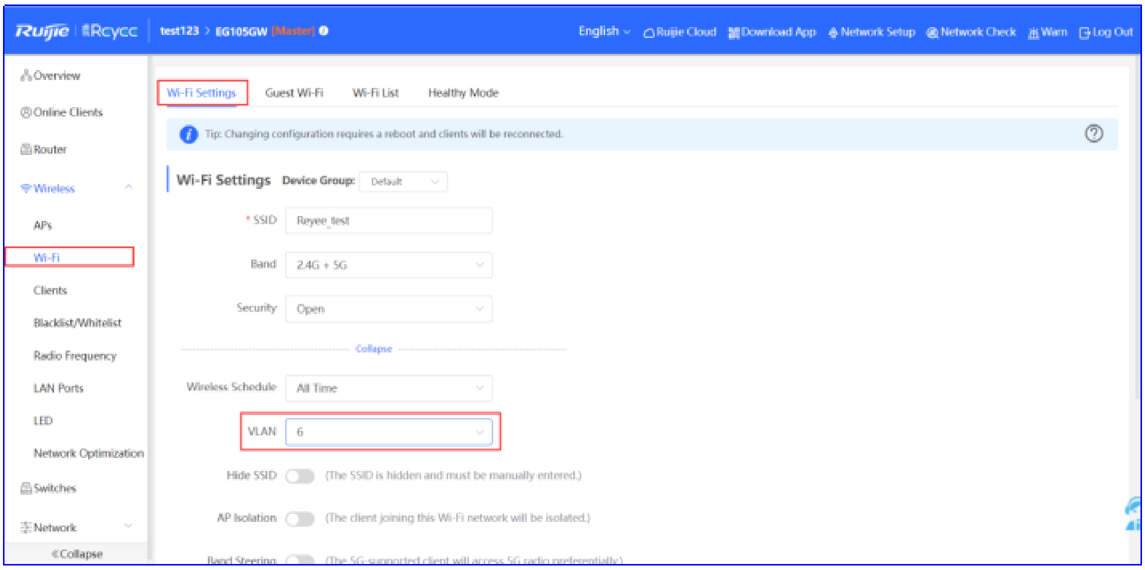
VLAN Settings

* Port: Select Type: Access

Permit: Select * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
5	Access	--	--	1
6	Access	--	--	1
7	Access	--	--	1
8	Access	--	--	1
9	Trunk	1,6	1	--

Step 3: Click **Wireless-> Wi-Fi -> Wi-Fi Settings,** Configure SSID named Reyee_test and set VLAN6 to this ssid.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: Reyee_test

Band: 2.4G + 5G

Security: Open

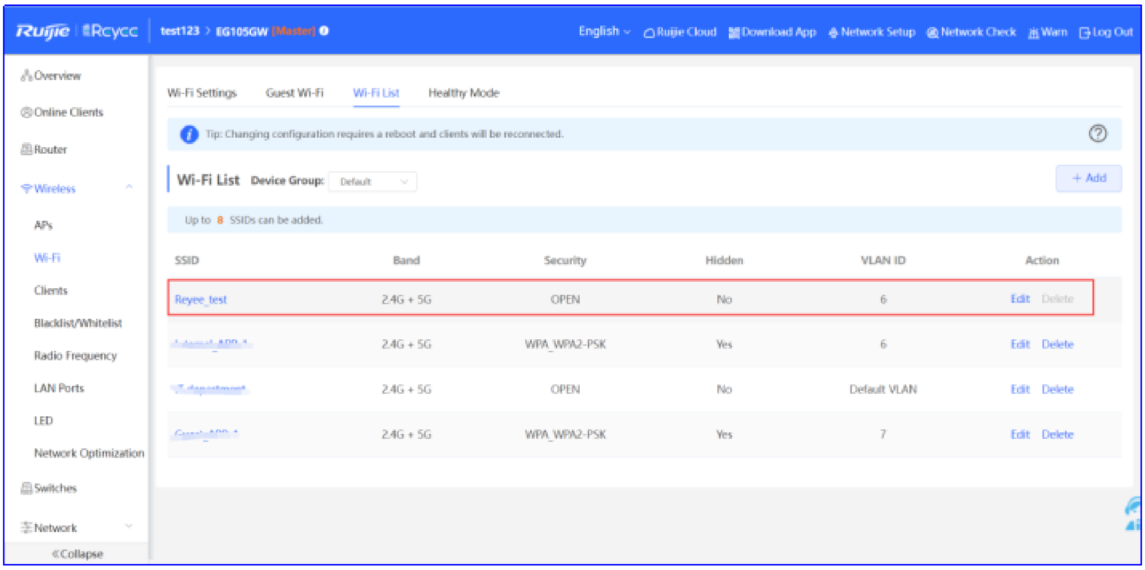
Wireless Schedule: All Time

VLAN: 6

Hide SSID (The SSID is hidden and must be manually entered.)

AP Isolation (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)



Tip: Changing configuration requires a reboot and clients will be reconnected.

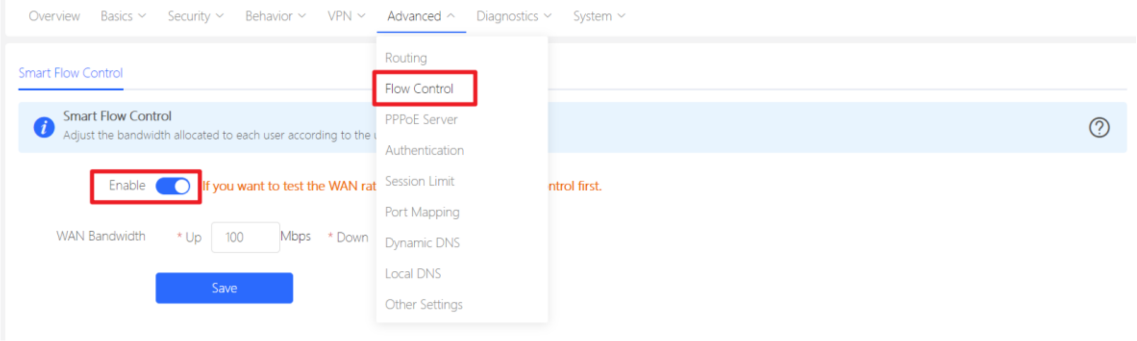
Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete
[redacted]	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete

2. Configure Smart Flow Control

Step 1: Choose **Router** → **Advanced** → **Flow Control** and enable **Smart flow control** feature.



Overview Basics Security Behavior VPN Advanced Diagnostics System

Routing
Flow Control
PPPoE Server
Authentication
Session Limit
Port Mapping
Dynamic DNS
Local DNS
Other Settings

Smart Flow Control

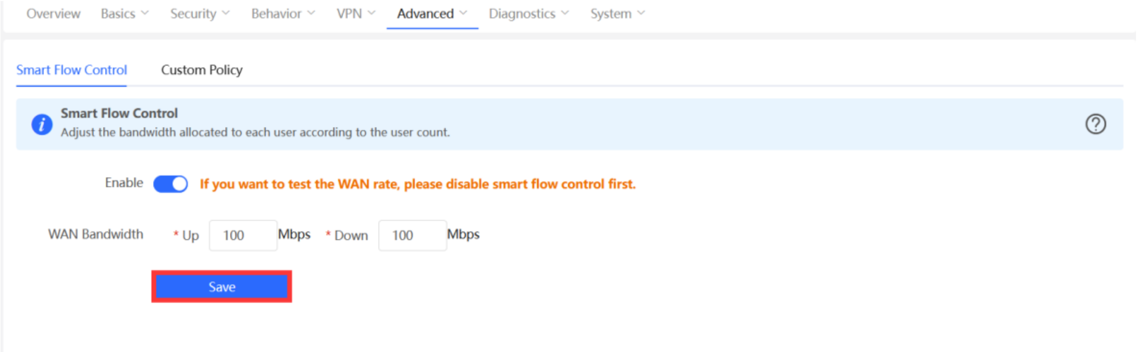
Smart Flow Control
Adjust the bandwidth allocated to each user according to the

Enable If you want to test the WAN rat ntrol first.

WAN Bandwidth * Up 100 Mbps * Down

Save

Step 2: Fill in the uplink and downlink WAN bandwidth as 100Mbps and **Save** the configuration.



Overview Basics Security Behavior VPN Advanced Diagnostics System

Smart Flow Control Custom Policy

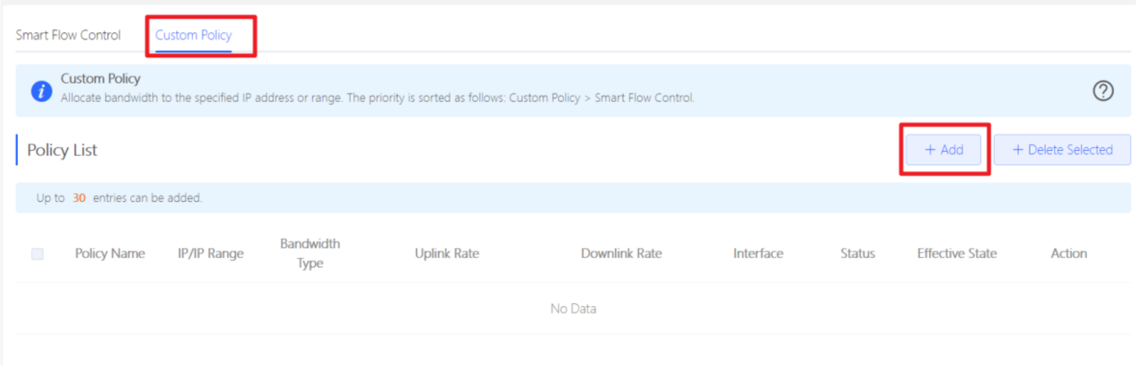
Smart Flow Control
Adjust the bandwidth allocated to each user according to the user count.

Enable If you want to test the WAN rate, please disable smart flow control first.

WAN Bandwidth * Up 100 Mbps * Down 100 Mbps

Save

Step 3: After step2 is being done, **Custom Policy** will be displayed. Click **Add** to add policy.



Smart Flow Control Custom Policy

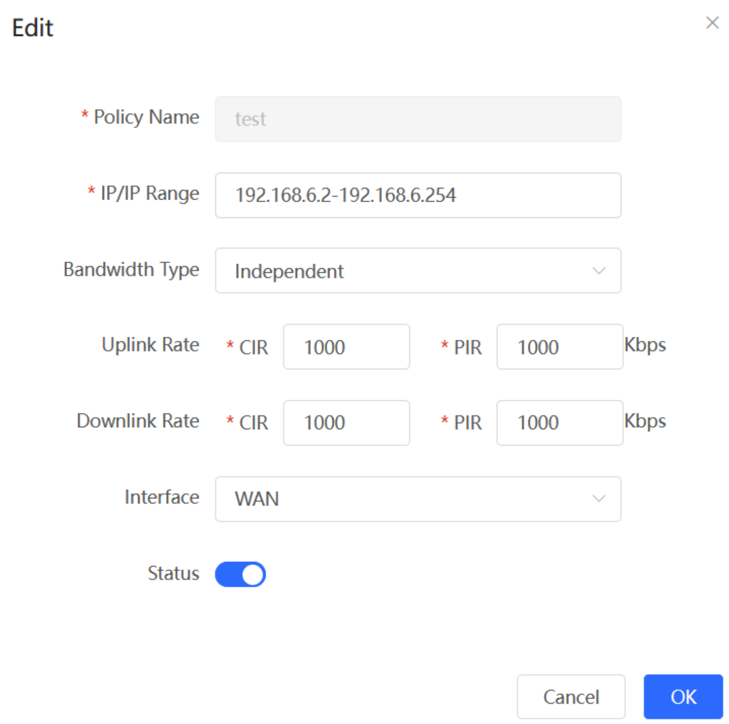
Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List + Add + Delete Selected

Up to 30 entries can be added.

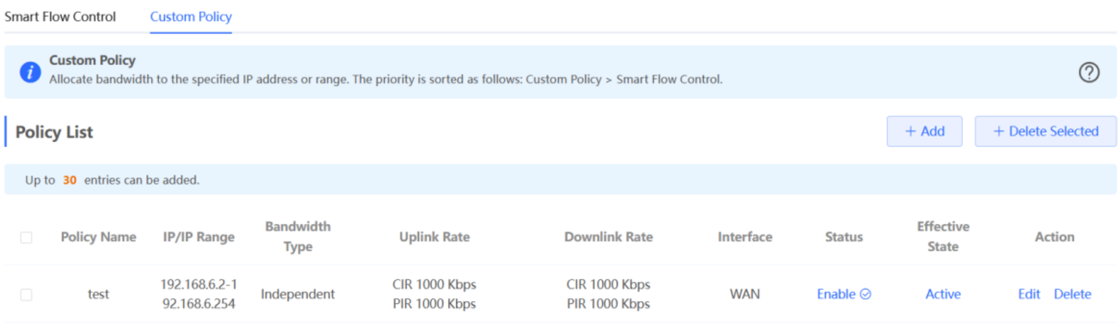
□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
					No Data				

Step 4: Set **Policy Name**, **IP range**, **Bandwidth Type**, **Rate**, etc.



Edit

* Policy Name	test
* IP/IP Range	192.168.6.2-192.168.6.254
Bandwidth Type	Independent
Uplink Rate	* CIR 1000 * PIR 1000 Kbps
Downlink Rate	* CIR 1000 * PIR 1000 Kbps
Interface	WAN
Status	●



Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List

Up to 30 entries can be added.

□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	192.168.6.2-1 92.168.6.254	Independent	CIR 1000 Kbps PIR 1000 Kbps	CIR 1000 Kbps PIR 1000 Kbps	WAN	Enable ✓	Active	Edit Delete

Note:

Bandwidth Type:

1) Shared: Shared indicates that all IP addresses share with the total bandwidth.

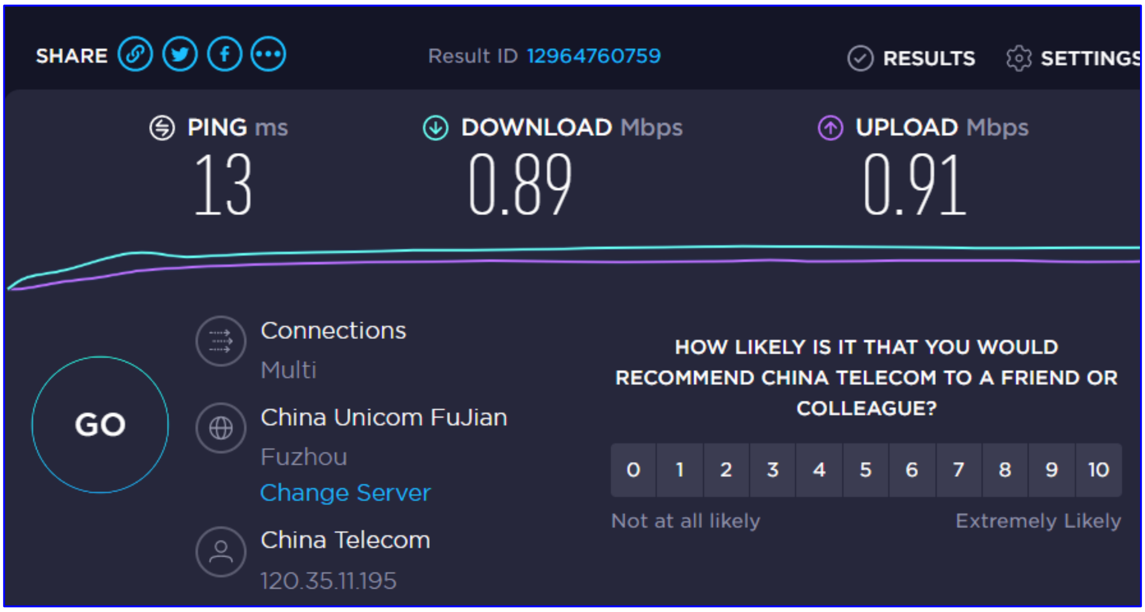
2) Indenpended: Independent indicates that the rate limit is setted for per IP address.

CIR: CIR means committed information rate.

PIR: PIR means peak information rate.

Configuration Verification

Use Speed test tool to check that each user is limited up to 1Mbps.



Result ID 12964760759

PING ms 13

DOWNLOAD Mbps 0.89

UPLOAD Mbps 0.91

Connections Multi

China Unicom FuJian Fuzhou

Change Server

China Telecom 120.35.11.195

HOW LIKELY IS IT THAT YOU WOULD RECOMMEND CHINA TELECOM TO A FRIEND OR COLLEAGUE?

0 1 2 3 4 5 6 7 8 9 10

Not at all likely Extremely Likely

20.2 Reyee Cloud Authentication Solution

20.2.1 Working Principle

Cloud authentication allows you to control users accessing to the wireless network. The configuration will be synchronized from Cloud to local EG device. In portal authentication, all the client’s HTTP requests will be redirected to an authentication page first. The clients are required to authenticate, payment, accept the end-user license agreement, acceptable use policy, survey completion, or other valid credentials, then they can visit the internet after the authentication succeeded.

20.2.2 Application Scenario

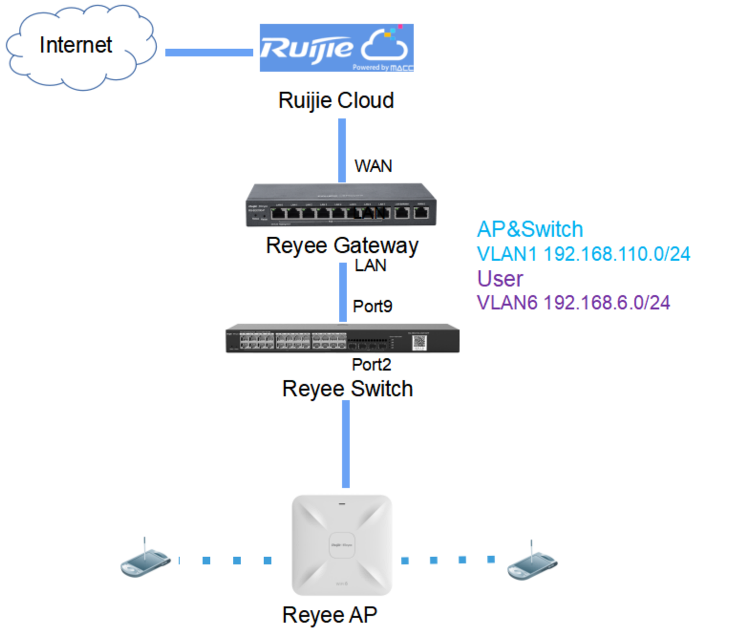
Portal authentication, also known as Web authentication, is usually deployed in a guest-access network (like a hotel or a coffee shop) to control the client’s internet access.

20.2.3 Configuration Case

Requirement

Users are required to authenticate first before allowed to access the Internet. Reyee AP can’t support cloud authentication, need Reyee EG to do that.

Network Topology



Network Description:

EG works as a DHCP server to assign IP addresses to users and AP& switch devices

The AP& switch devices obtain the IP address 192.168.110.0/24 in the VLAN1 network segment for Internet access

The users obtain the IP address 192.168.6.0/24 in the VLAN6 network segment for Internet access

The Ruijie Cloud work as platform to manage and monitor devices and clients status and provide captive authentication for clients.

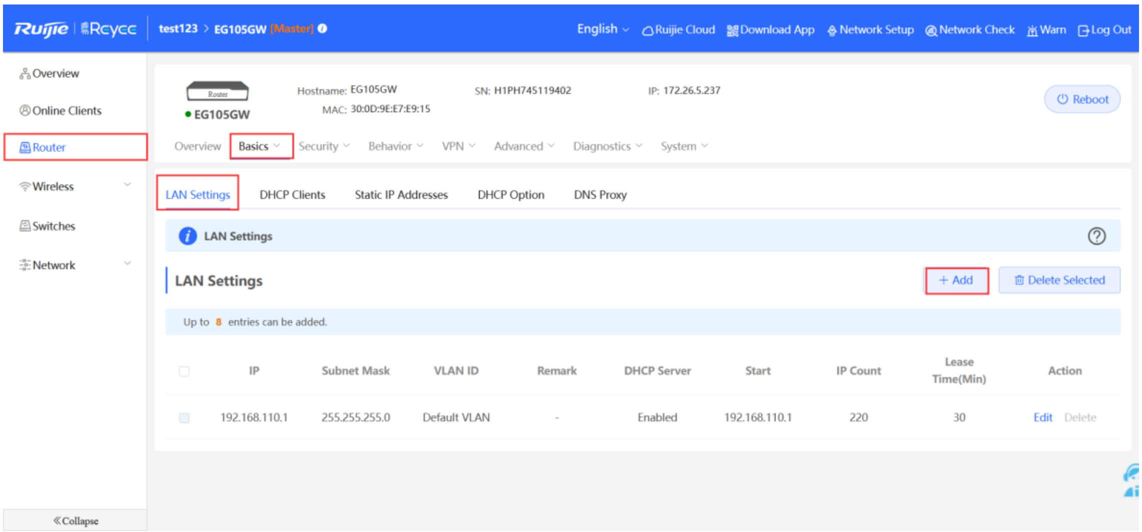
Configuration Steps

Configure basic network

Configure cloud authentication

1. Configure basic network

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN1 and VLAN6 network segment on the EG.



EG105GW

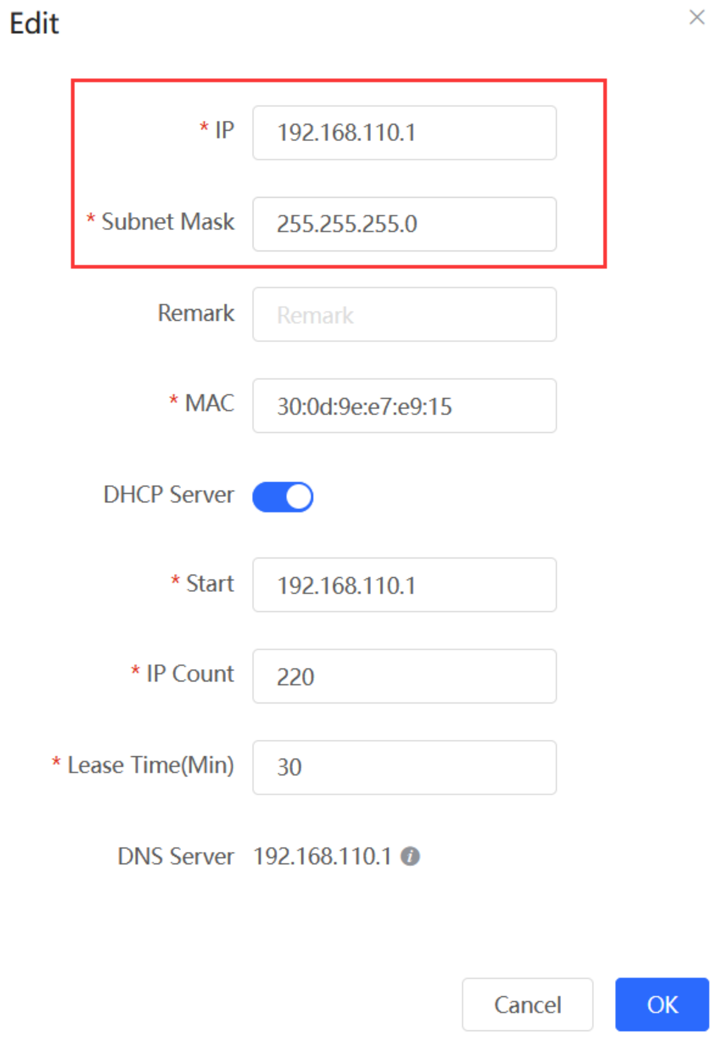
Hostname: EG105GW MAC: 30:0D:9E:E7:E9:15 SN: H1PH745119402 IP: 172.26.5.237

LAN Settings

LAN Settings

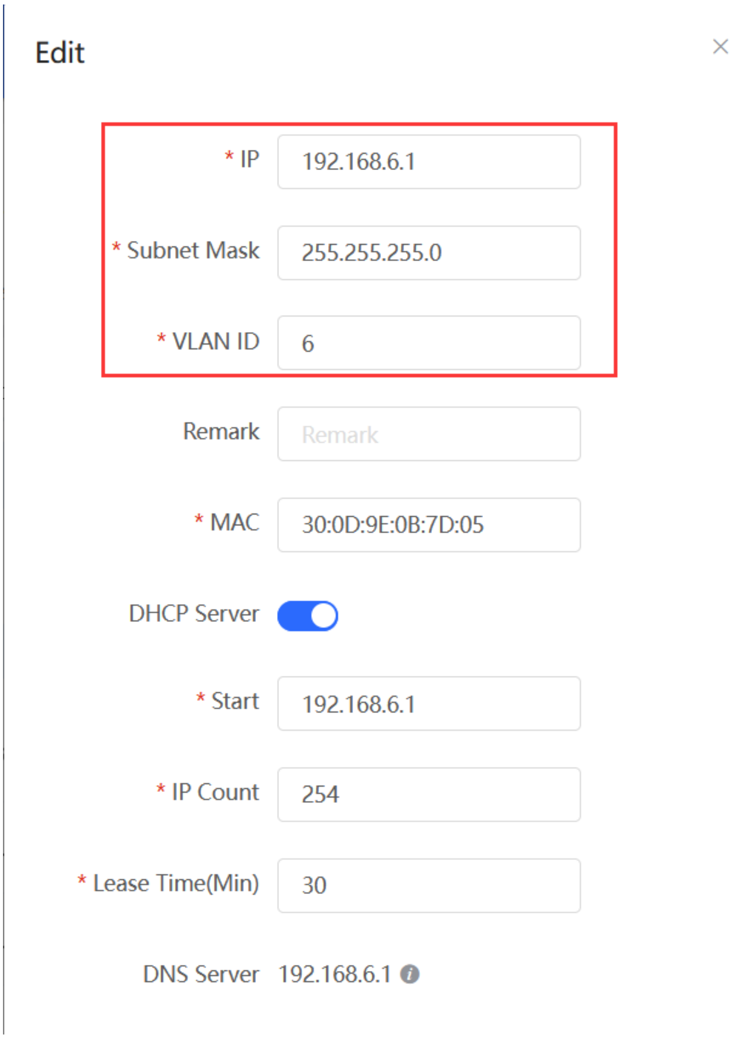
Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete



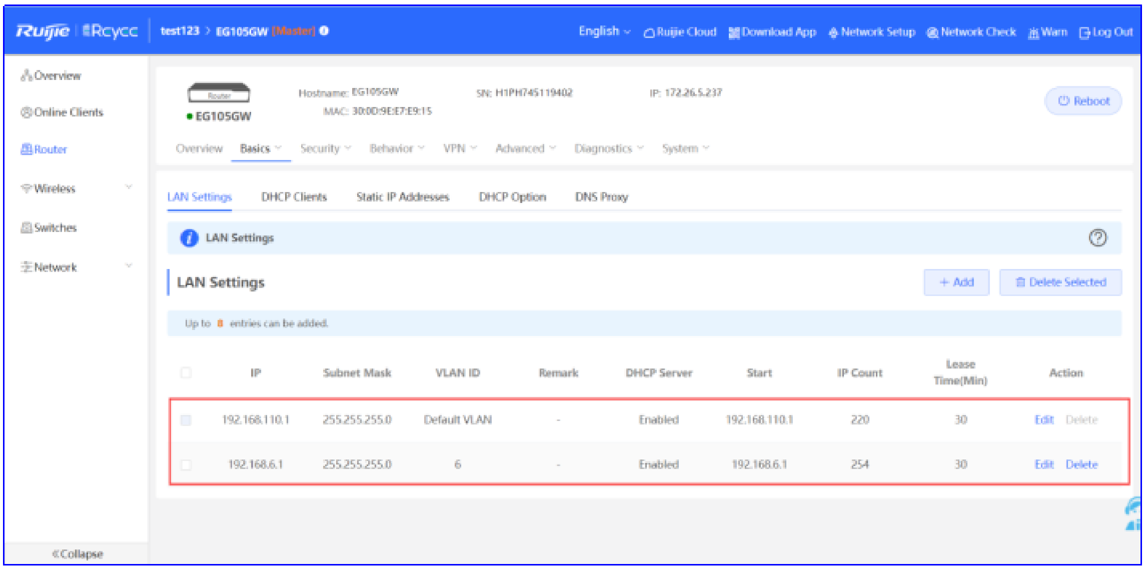
Edit

* IP	192.168.110.1
* Subnet Mask	255.255.255.0
Remark	Remark
* MAC	30:0d:9e:e7:e9:15
DHCP Server	●
* Start	192.168.110.1
* IP Count	220
* Lease Time(Min)	30
DNS Server	192.168.110.1



Edit

* IP	192.168.6.1
* Subnet Mask	255.255.255.0
* VLAN ID	6
Remark	Remark
* MAC	30:0D:9E:0B:7D:05
DHCP Server	●
* Start	192.168.6.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.6.1



EG105GW

Hostname: EG105GW SN: H1PH745119402 IP: 172.26.5.237

MAC: 30:0D:9E:E7:E9:15

LAN Settings

LAN Settings

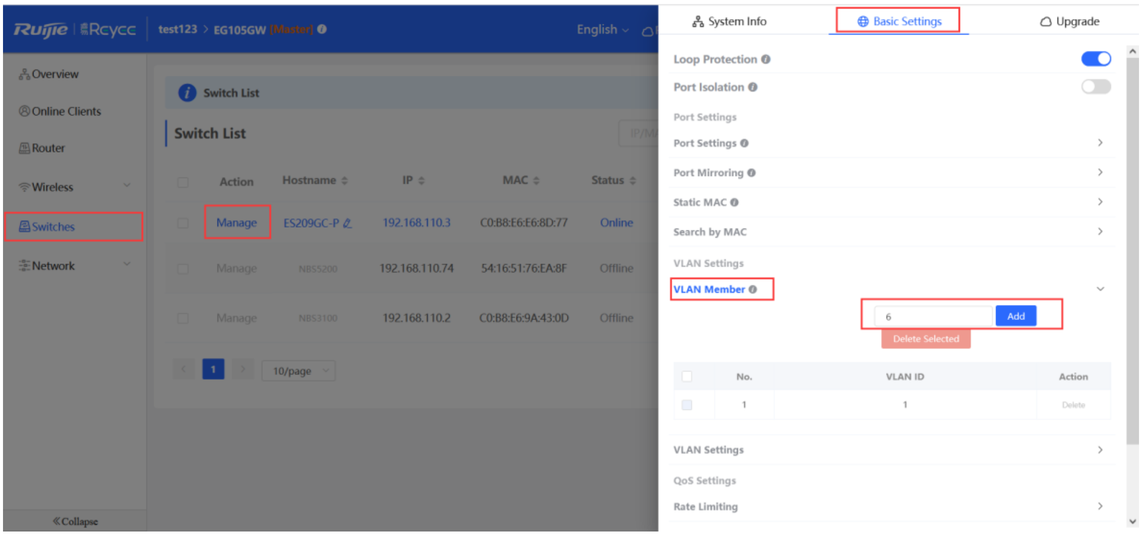
Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete

Note:

Default VLAN network is set to 192.168.110.0/24 network segment.

Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN6 on the switch, and click **VLAN Settings** to set port 2 and port 9 to trunk port which connect to AP and EG and allow VLAN 1 and VLAN 6 to pass through, then check the port settings on the device.



Switch List

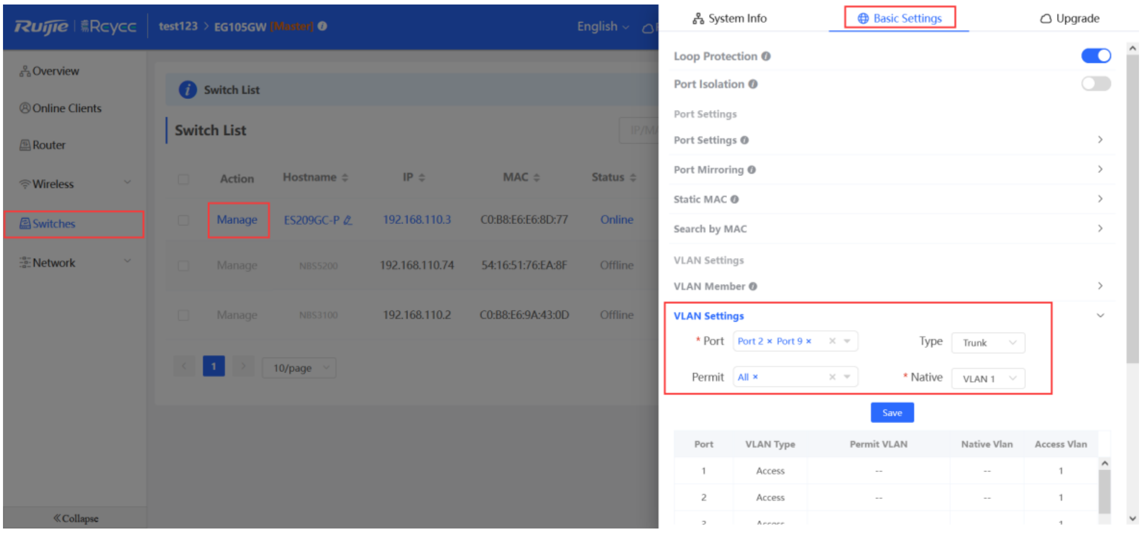
Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member

6

No.	VLAN ID	Action
1	1	Delete

VLAN Settings
QoS Settings
Rate Limiting



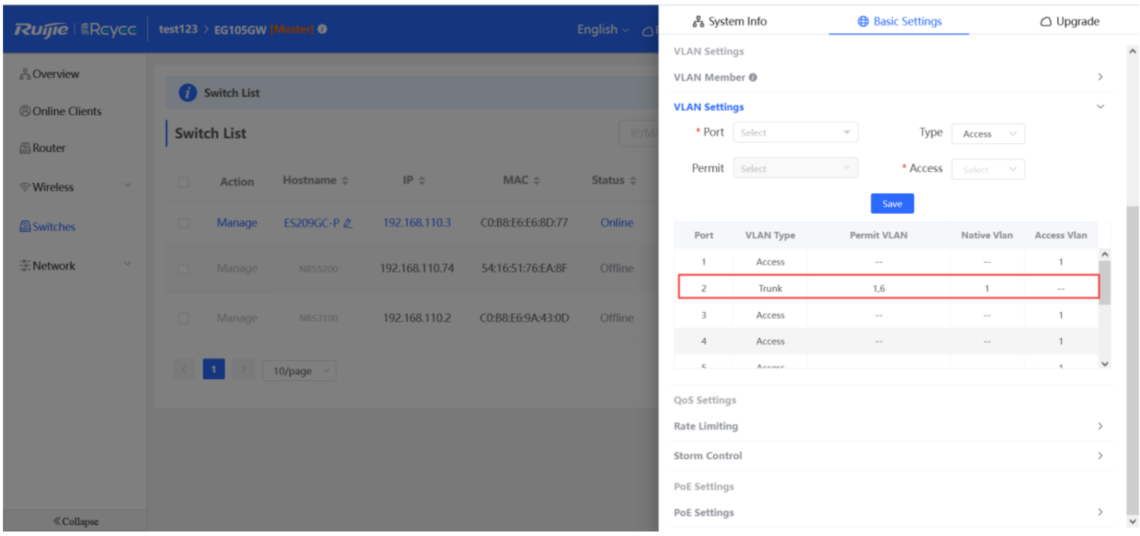
Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
VLAN Settings

* Port: Port 2 × Port 9 × Type: Trunk
Permit: All × * Native: VLAN 1

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Access	--	--	1



Switch List

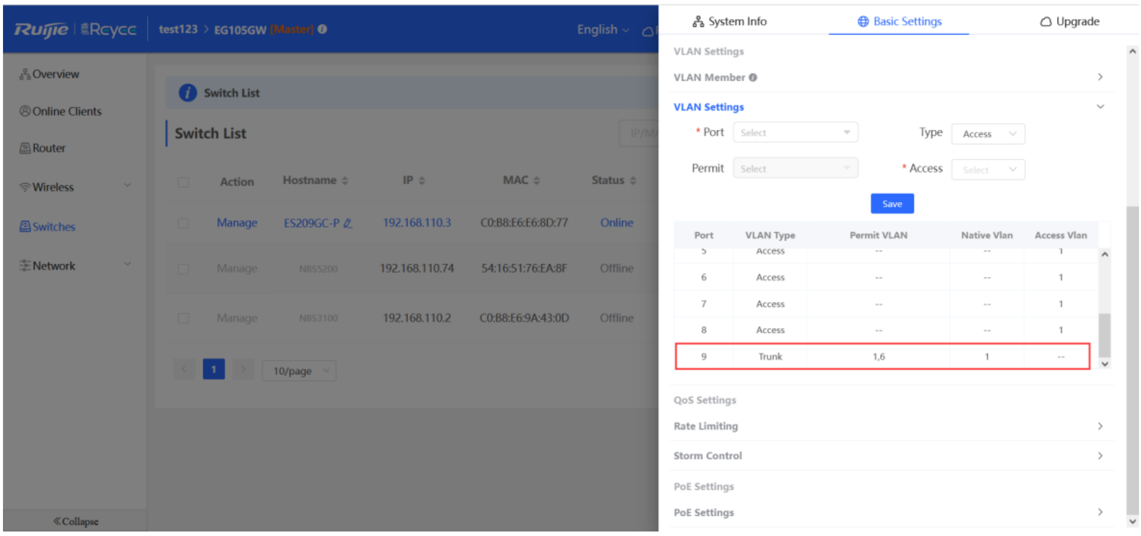
Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

VLAN Settings
VLAN Member
VLAN Settings

* Port: Select Type: Access
Permit: Select * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6	1	--
3	Access	--	--	1
4	Access	--	--	1

QoS Settings
Rate Limiting
Storm Control
PoE Settings
PoE Settings



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

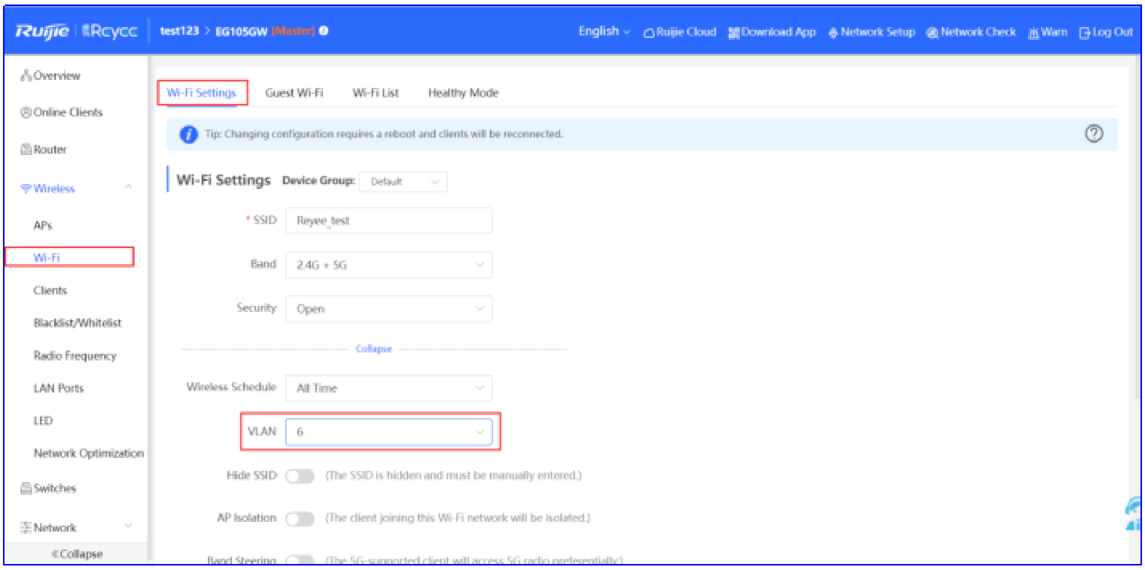
VLAN Settings

* Port: Select Type: Access

Permit: Select * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
5	Access	--	--	1
6	Access	--	--	1
7	Access	--	--	1
8	Access	--	--	1
9	Trunk	1,6	1	--

Step 3: Click **Wireless** -> **Wi-Fi** -> **Wi-Fi Settings, c**onfigure a SSID named as Reyee test and set VLAN6 to this SSID.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: Reyee_test

Band: 2.4G + 5G

Security: Open

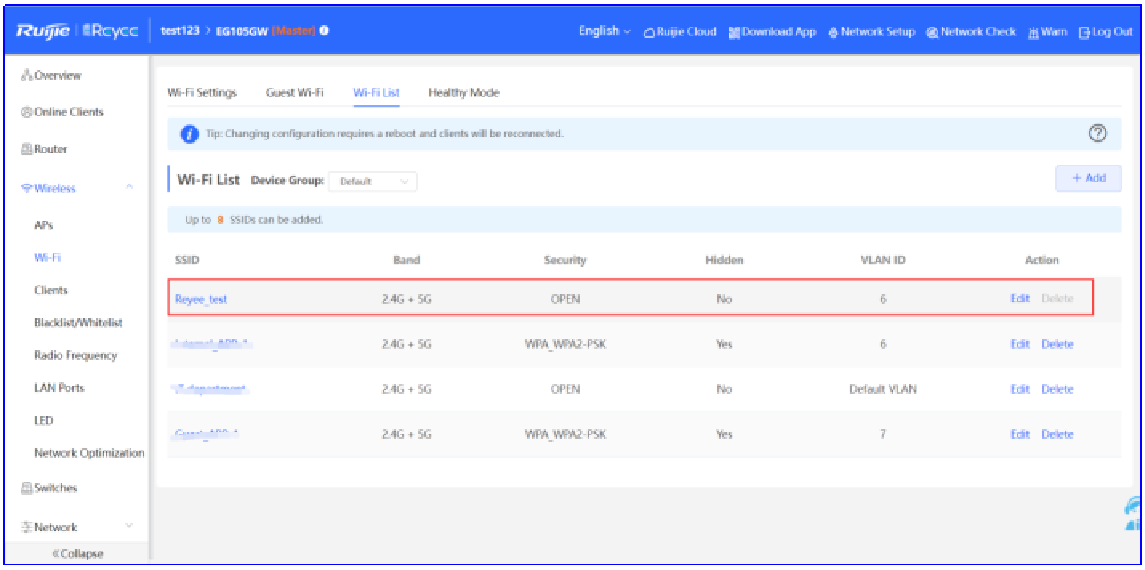
Wireless Schedule: All Time

VLAN: 6

Hide SSID (The SSID is hidden and must be manually entered.)

AP Isolation (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)



Tip: Changing configuration requires a reboot and clients will be reconnected.

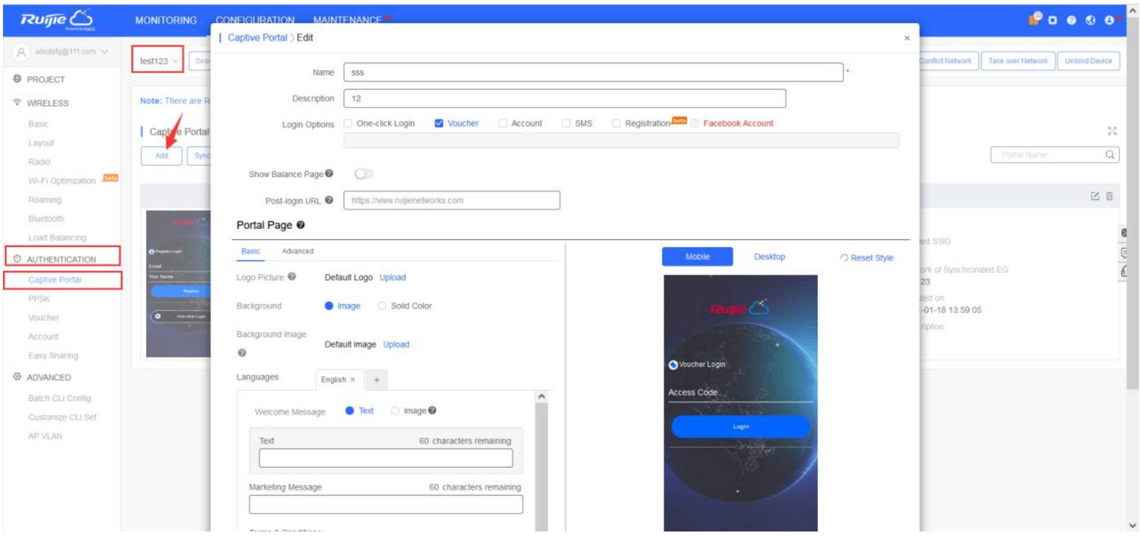
Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete
[redacted]	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete

Configure cloud authentication

Step 1: Select **CONFIGURATION** -> **AUTHENTICATION** -> **Captive Portal** to open the Captive Portal page, and click **Add** to create a new portal template and edit the captive portal template.



Captive Portal > Edit

Name: sss

Description: 12

Login Options: □ One-click Login ☑ Voucher □ Account □ SMS □ Registration □ Facebook Account

Show Balance Page: off

Post-login URL: https://www.ruijienetworks.com

Portal Page

Basic | Advanced

Logo Picture: Default Logo Upload

Background: ● Image ○ Solid Color

Background Image: Default Image Upload

Languages: English

Welcome Message: ● Text ○ Image

Text: 60 characters remaining

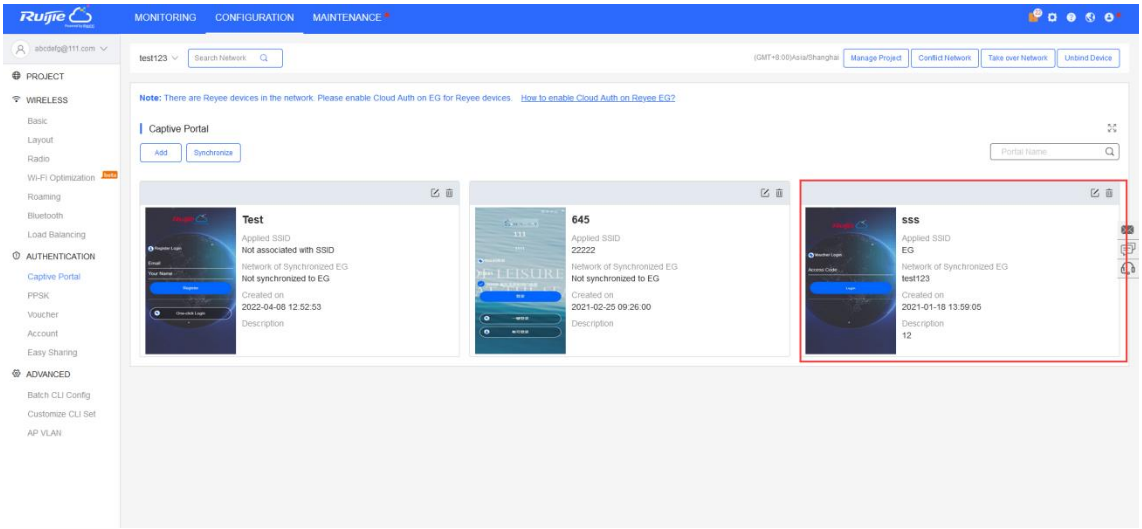
Marketing Message: 60 characters remaining

Mobile | Desktop | Reset Style

Voucher Login

Access Code

Login



Note: There are Reyee devices in the network. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?

Captive Portal

Test
Applied SSID: Not associated with SSID
Network of Synchronized EG: Not synchronized to EG
Created on: 2022-04-08 12:52:53
Description

645
Applied SSID: 22222
Network of Synchronized EG: Not synchronized to EG
Created on: 2021-02-25 09:26:00
Description

sss
Applied SSID: EG
Network of Synchronized EG: test123
Created on: 2021-01-18 13:59:05
Description: 12

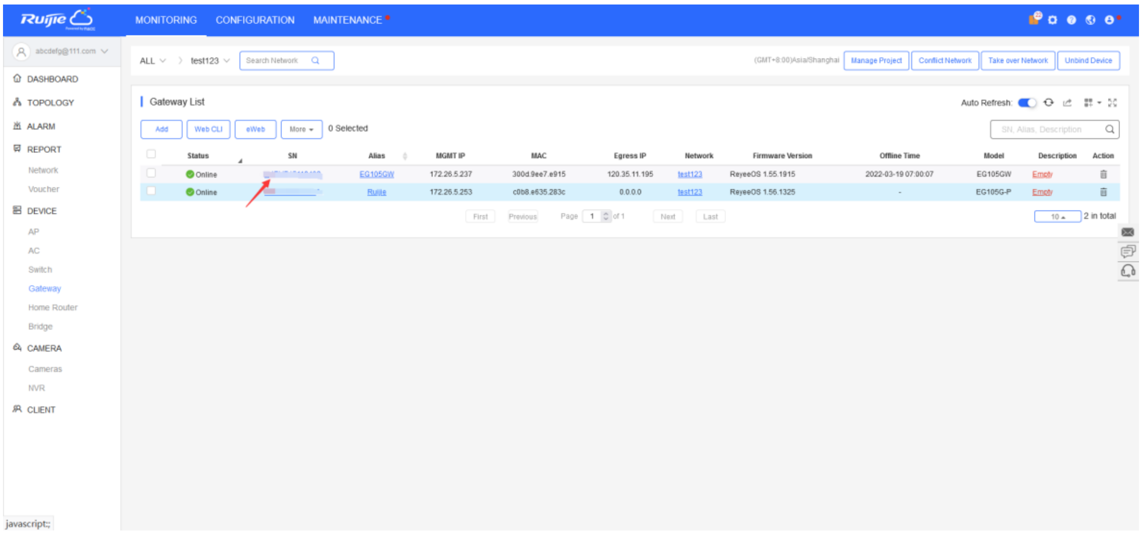
Note:

One-click Login: Login without username and password. Support to set the Access Duration and Access Times per day.

Voucher: Login with a random eight-digit password.

Account: Login with the account and password.

Step 2: Make sure the Reyee EG is online on Ruijie Cloud and click its SN in the list to enter the configure page



(GMT+8:00)Asia/Shanghai

Gateway List

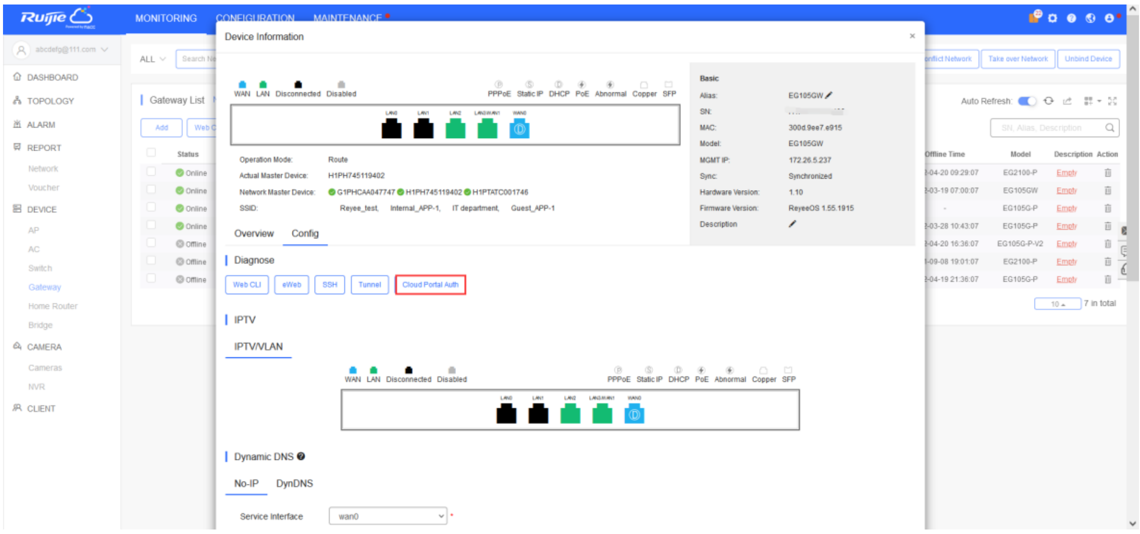
Auto Refresh: ●

0 Selected

Status	SN	Alias	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Action
Online	[redacted]	EG105GW	172.26.5.237	300d.9ee7.e915	120.35.11.195	test123	ReyeeOS 1.55.1915	2022-03-19 07:00:07	EG105GW	Empty	🗑
Online	[redacted]	Ruijie	172.26.5.253	c0b8.e635.283c	0.0.0.0	test123	ReyeeOS 1.56.1325	-	EG105G-P	Empty	🗑

Page 1 of 1 10 2 in total

Step 3: Click **Cloud portal Auth** to configure the authentication on Cloud



Device Information

Operation Mode: Route

Actual Master Device: H1PH745119402

Network Master Device: G1PHCAA047747 H1PH745119402 H1PTATC001746

SSID: Reyee_test, Internal_APP-1, IT department, Guest_APP-1

Basic

Alias: EG105GW

SN: [redacted]

MAC: 300d.9ee7.e915

Model: EG105GW

MGMT IP: 172.26.5.237

Sync: Synchronized

Hardware Version: 1.10

Firmware Version: ReyeeOS 1.55.1915

Description

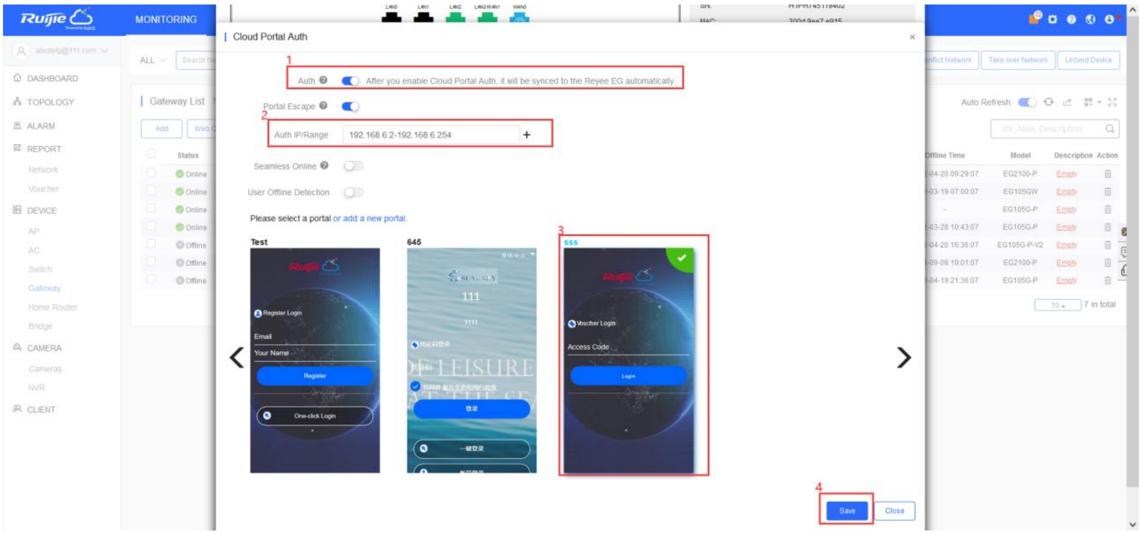
Diagnose

IPTV

Dynamic DNS

Service Interface: wan0

Step 4: Enable **Auth** firstly, then set **Auth IP Range 192.168.6.2-192.168.6.254** which need to authenticate and choose the portal template to be used. In the end, click **Save** to save all configurations.



Cloud Portal Auth

Auth ● After you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.

Portal Escape ●

Auth IP/Range: 192.168.6.2-192.168.6.254 +

Seamless Online ○

User Offline Detection ○

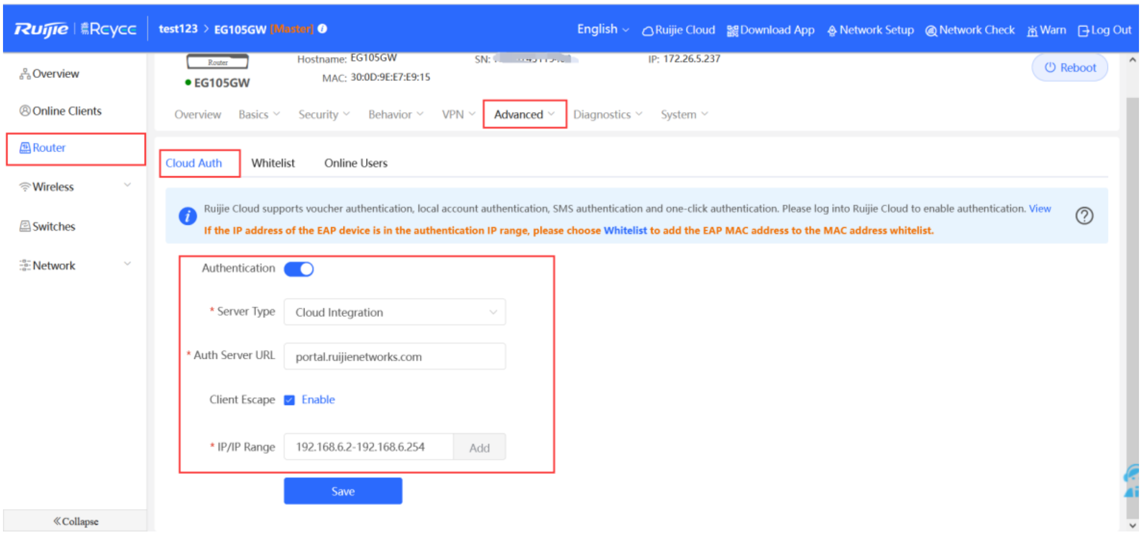
Please select a portal or add a new portal.

Note:

The EG, Switch and AP IP address needs to be excluded, otherwise the device will not be able to access the Internet.

Configuration Verification

Click **Router** -> **Advanced** -> **LAN** -> **Authentication** -> **Cloud Auth,** Check whether the configuration has been synchronized to EG.



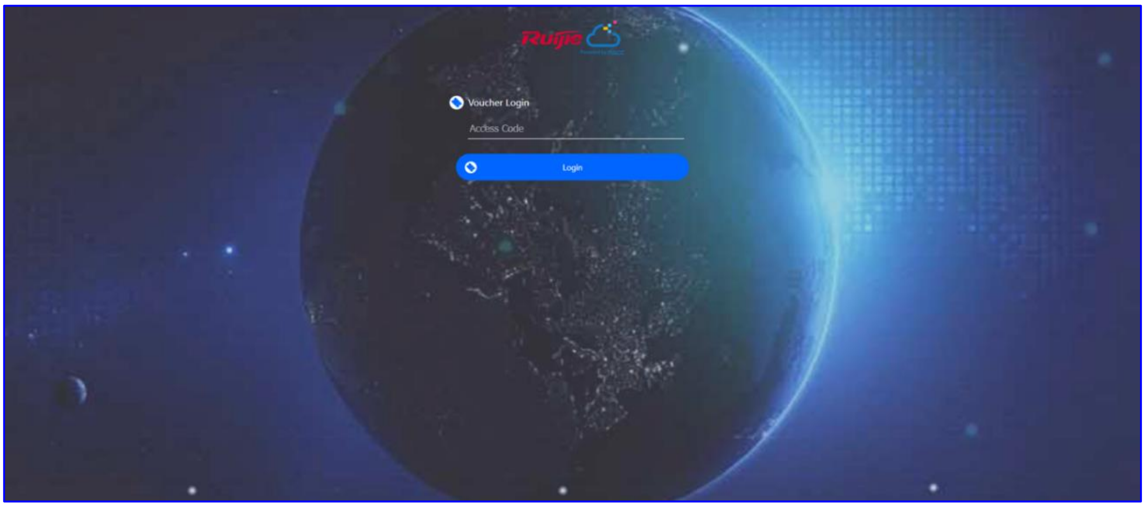
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: [redacted]
IP: 172.26.5.237

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

If the IP address of the EAP device is in the authentication IP range, please choose Whitelist to add the EAP MAC address to the MAC address whitelist.

Authentication: on
* Server Type: Cloud Integration
* Auth Server URL: portal.ruijienetworks.com
Client Escape: ☑ Enable
* IP/IP Range: 192.168.6.2-192.168.6.254 Add

Users which in 192.168.6.2-192.168.6.254 IP range are required to authenticate before accessing the Internet.



20.3 Reyee Guest WiFi Solution

20.3.1 Working Principle

Create a single internet entrance by using guest WiFi. The devices you allowed to access guest WiFi can access the internet but can’t access the home WiFi.

20.3.2 Application Scenario

Guest WiFi provides a secured Wi-Fi access for guests to share your home or office network. When someone visits your house, apartment, or workplace, you can enable the guest WiFi for them. You can set different access options for guest users, which is very effective to ensure the security and privacy of your main network.

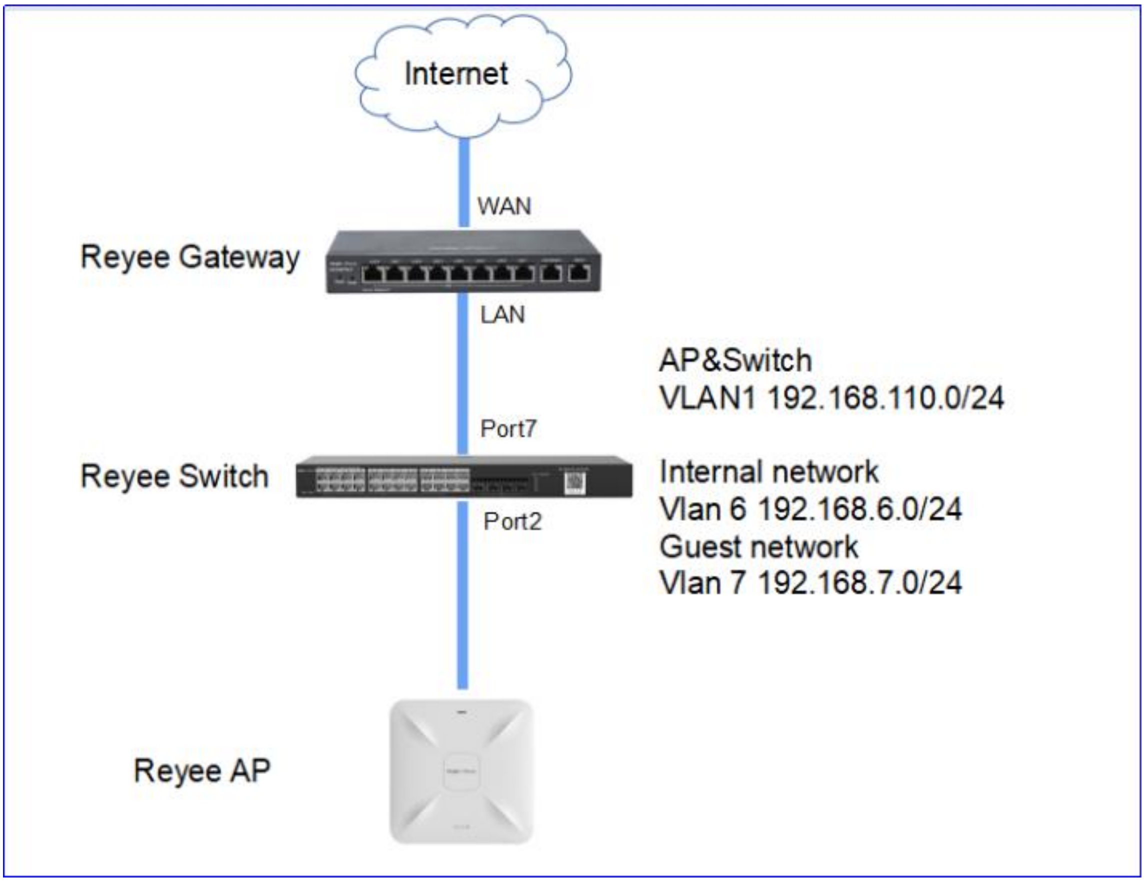
20.3.3 Configuration Case

1. **5.3.3.1 Configuration via EG’s eWeb**

Requirement

Configure Guest WiFi for the Guest users in the VLAN7 network segment and the users will cannot access the internal network in the VLAN6 network segment.

Network Topology



Network Description:

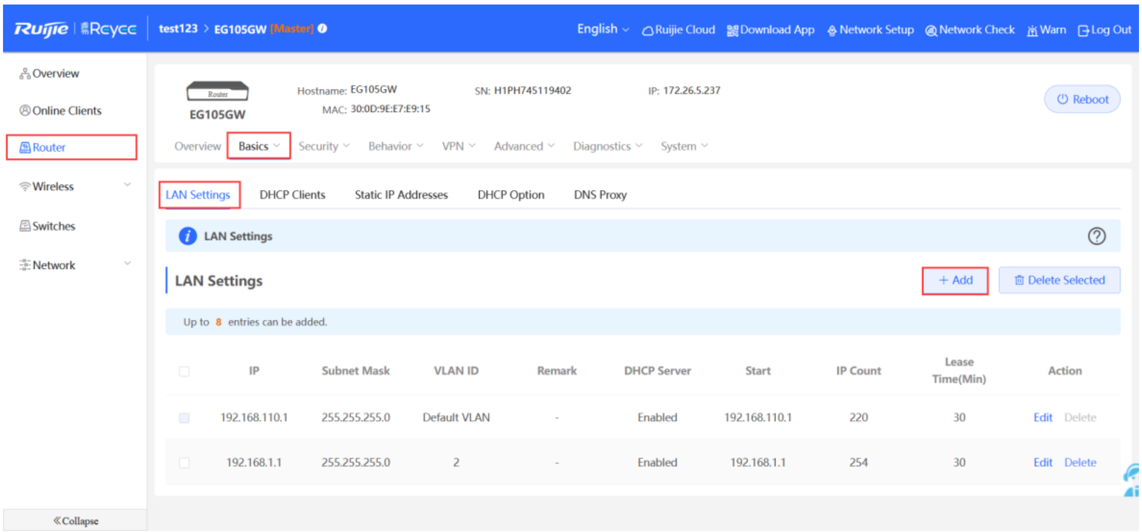
EG works as a DHCP server to assign IP addresses to users and AP & switch devices

The AP & switch devices obtain the IP address in the VLAN1 network segment for Internet access

The internal users obtain the IP address in the VLAN6 network segment for Internet access and the guest user obtain the IP address in the VLAN7 network segment for Internet access

Configuration Steps

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN 6 and VLAN 7 network segment on the EG



EG105GW

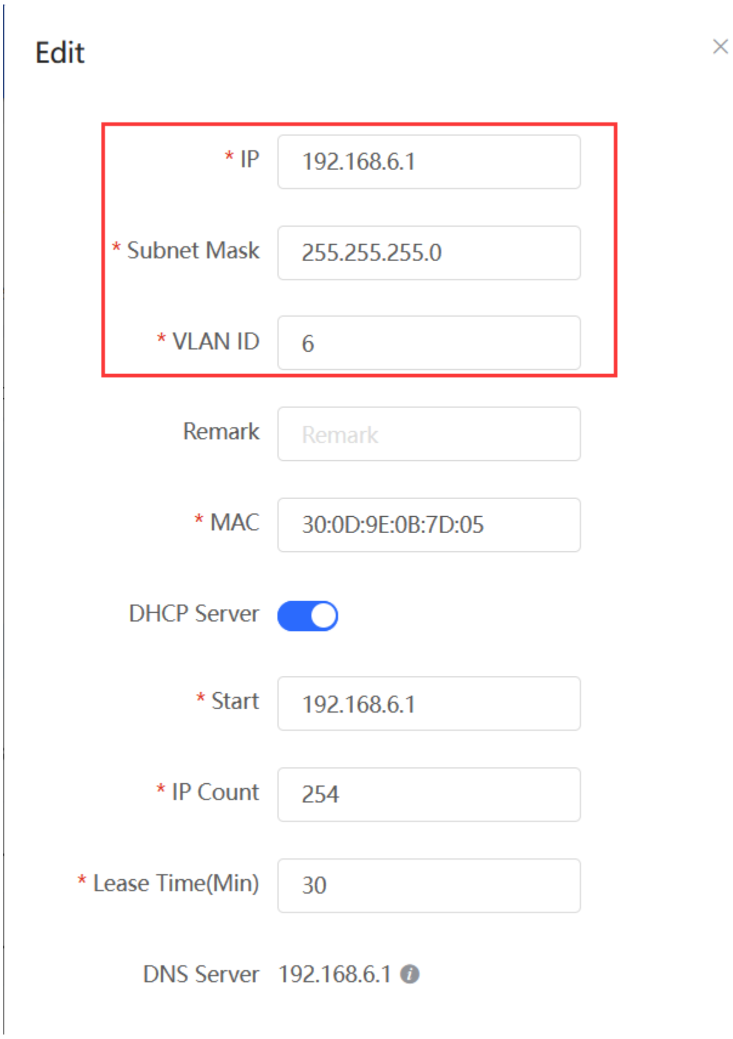
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237

LAN Settings

LAN Settings

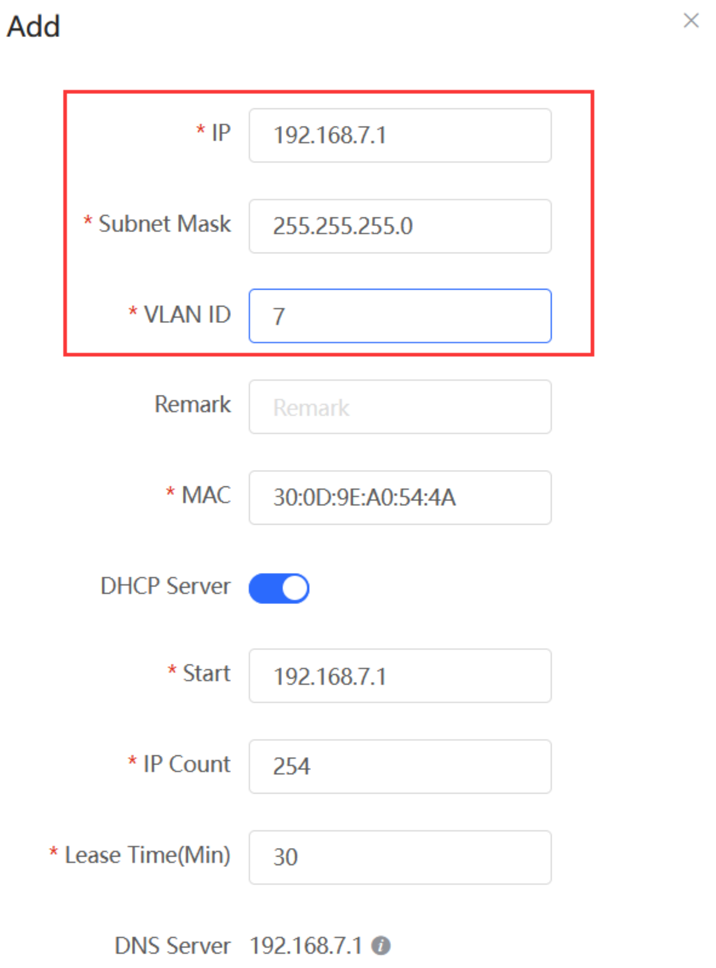
Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
□	192.168.1.1	255.255.255.0	2	-	Enabled	192.168.1.1	254	30	Edit Delete



Edit

* IP	192.168.6.1
* Subnet Mask	255.255.255.0
* VLAN ID	6
Remark	Remark
* MAC	30:0D:9E:0B:7D:05
DHCP Server	●
* Start	192.168.6.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.6.1



Add

* IP: 192.168.7.1

* Subnet Mask: 255.255.255.0

* VLAN ID: 7

Remark: Remark

* MAC: 30:0D:9E:A0:54:4A

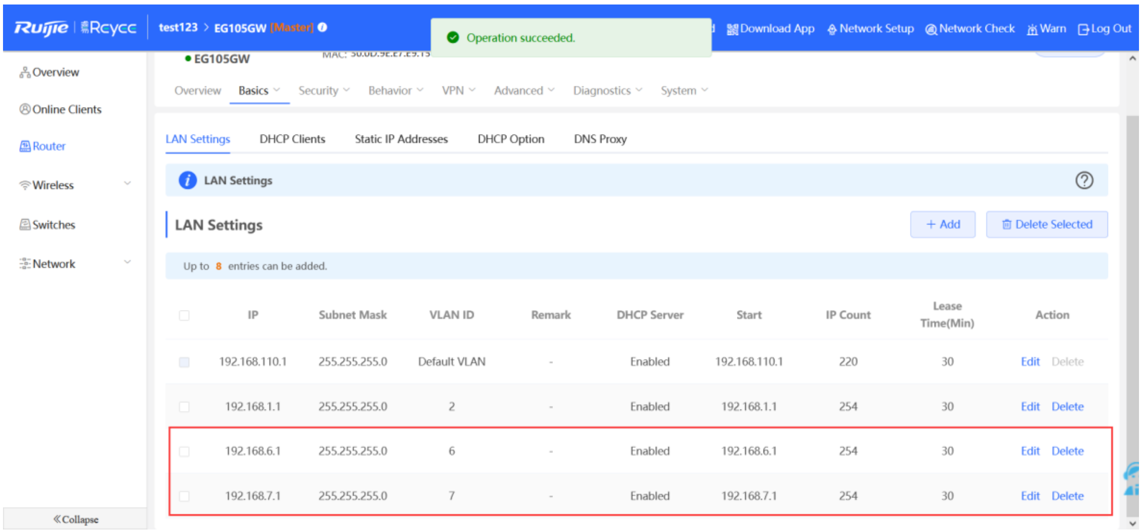
DHCP Server: On

* Start: 192.168.7.1

* IP Count: 254

* Lease Time(Min): 30

DNS Server: 192.168.7.1



Operation succeeded.

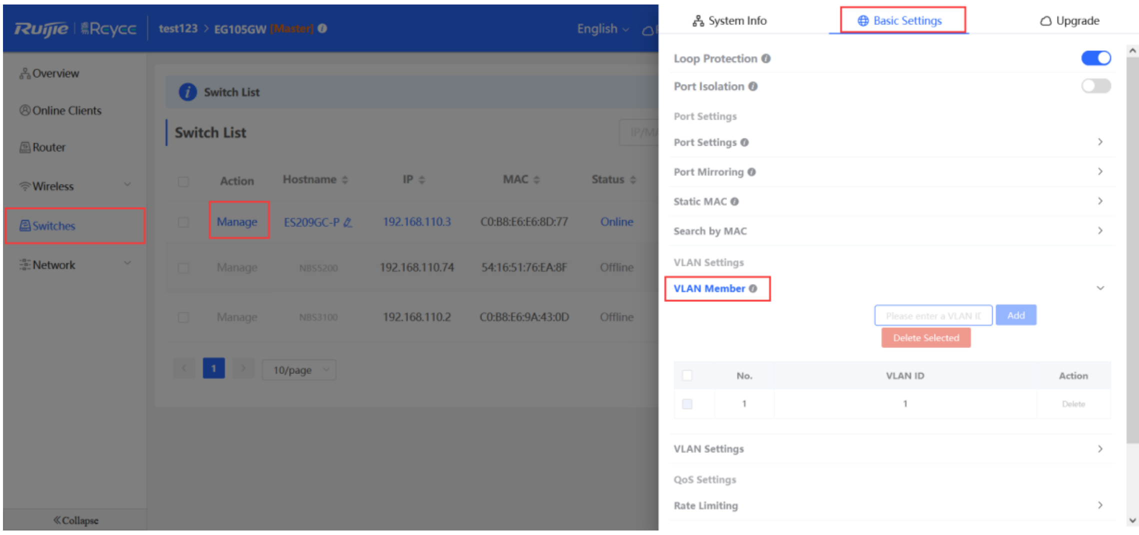
● EG105GW

LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	220	30	Edit Delete
□	192.168.1.1	255.255.255.0	2	-	Enabled	192.168.1.1	254	30	Edit Delete
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete

Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN 6 and VLAN 7 on the switch, and click **VLAN Settings** to set port 2 and port 7 to trunk port which connect to AP and EG and allow VLAN 1、VLAN 6 and VLAN 7 to pass through, then check the port settings on the device.



Switch List

□	Action	Hostname	IP	MAC	Status
□	Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
□	Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
□	Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

Loop Protection
Port Isolation

Port Settings
- Port Settings
- Port Mirroring
- Static MAC
- Search by MAC

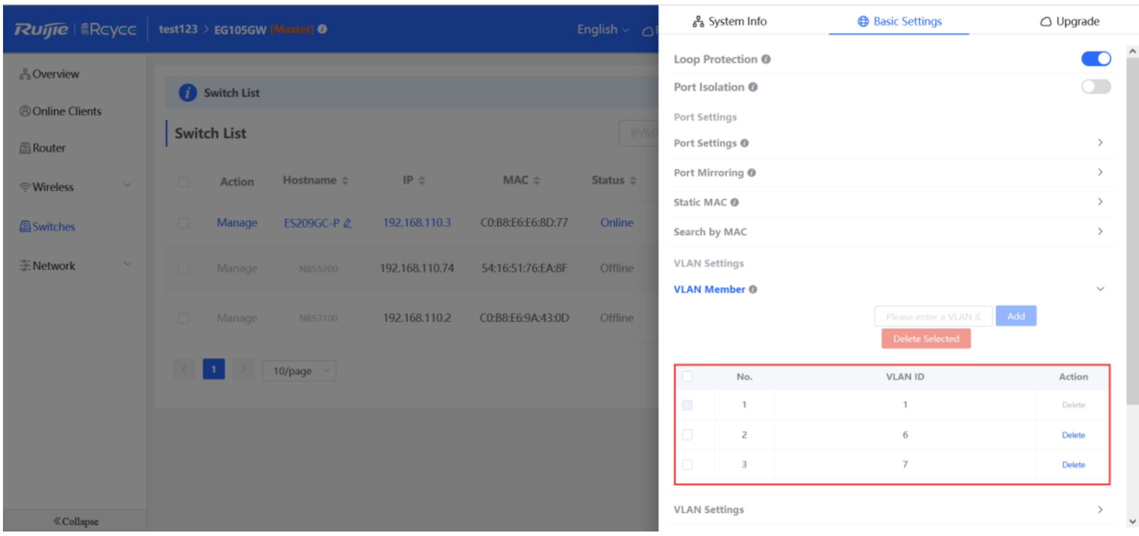
VLAN Settings
- VLAN Member

Please enter a VLAN ID | Add | Delete Selected

□	No.	VLAN ID	Action
□	1	1	Delete

- VLAN Settings

QoS Settings
- Rate Limiting



Switch List

□	Action	Hostname	IP	MAC	Status
□	Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
□	Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
□	Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

Loop Protection
Port Isolation

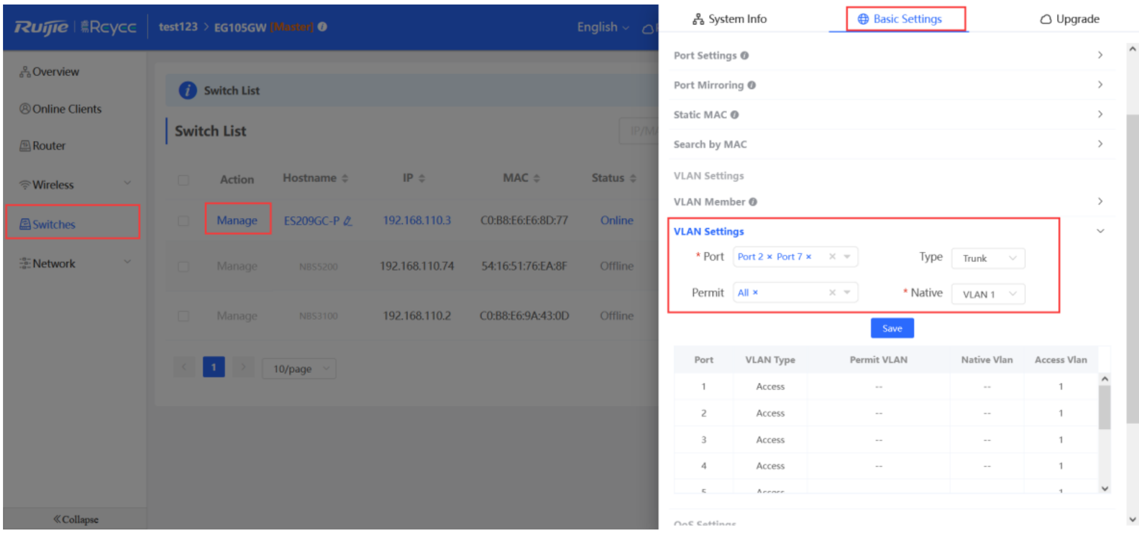
Port Settings
- Port Settings
- Port Mirroring
- Static MAC
- Search by MAC

VLAN Settings
- VLAN Member

Please enter a VLAN ID | Add | Delete Selected

□	No.	VLAN ID	Action
□	1	1	Delete
□	2	6	Delete
□	3	7	Delete

- VLAN Settings



Switch List

□	Action	Hostname	IP	MAC	Status
□	Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
□	Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
□	Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

1 10/page

- Port Settings
- Port Mirroring
- Static MAC
- Search by MAC

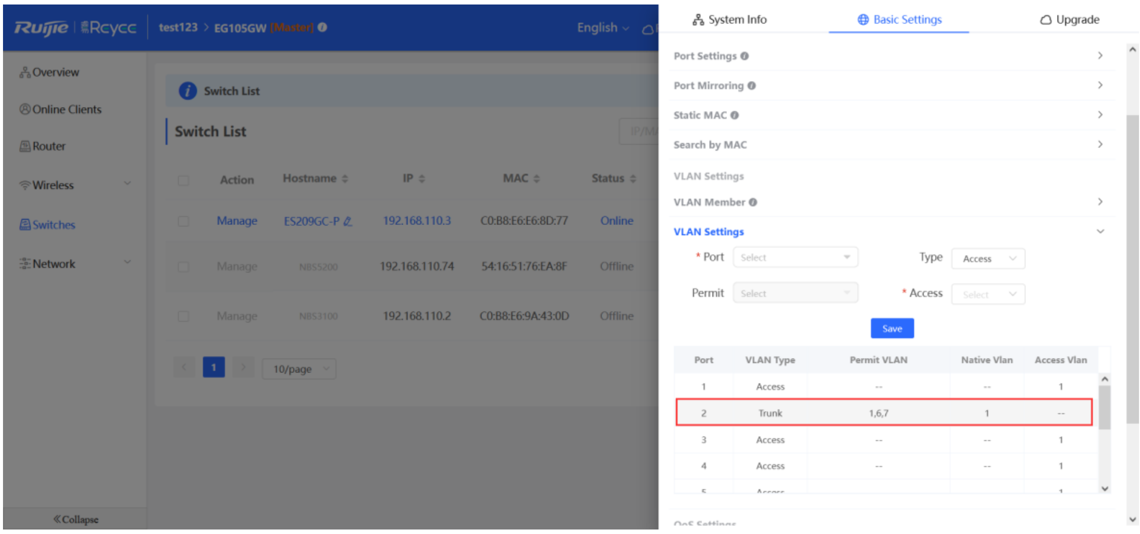
VLAN Settings
- VLAN Member
- VLAN Settings

* Port: Port 2 × Port 7 ×
Type: Trunk
Permit: All ×
* Native: VLAN 1

Save

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Access	--	--	1
3	Access	--	--	1
4	Access	--	--	1
5	Access			1

QoS Settings



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

10/page

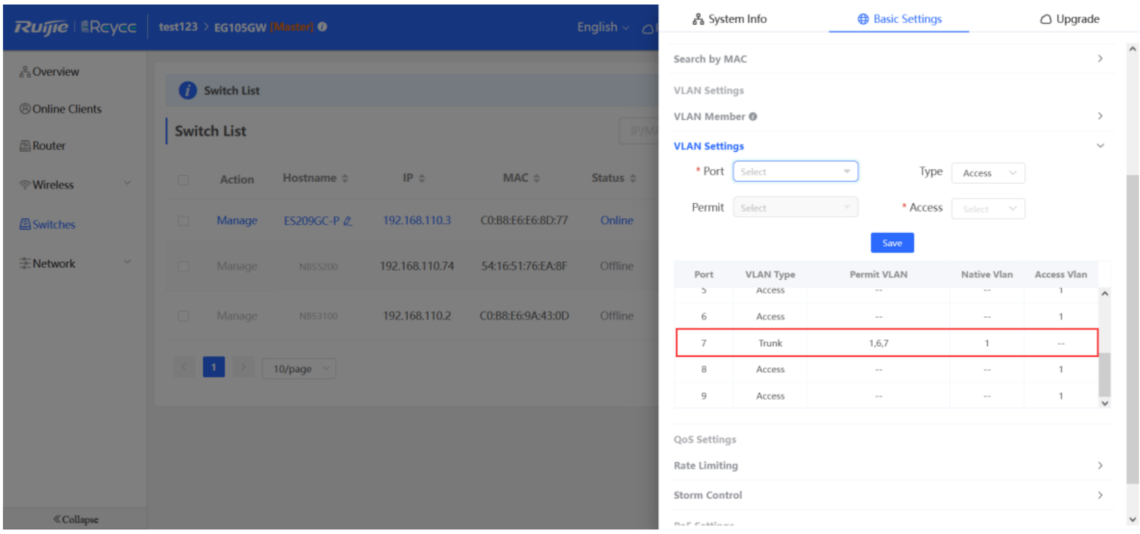
VLAN Settings

* Port: Select　Type: Access

Permit: Select　* Access: Select

Save

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6,7	1	--
3	Access	--	--	1
4	Access	--	--	1
5	Access			1



Switch List

Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

10/page

VLAN Settings

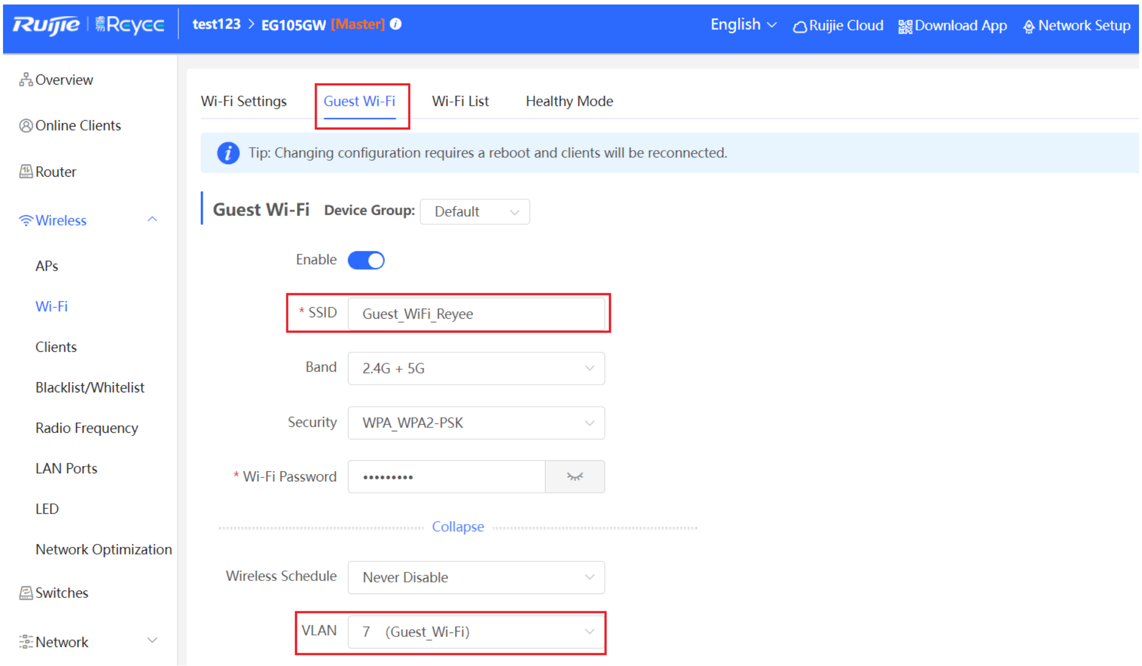
* Port: Select　Type: Access

Permit: Select　* Access: Select

Save

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
5	Access	--	--	1
6	Access	--	--	1
7	Trunk	1,6,7	1	--
8	Access	--	--	1
9	Access	--	--	1

Step 3: Click **Wireless-> Wi-Fi -> Guest WiFi, c**onfigure a Guest WiFi SSID named as Guest_WiFi_Reyee and set VLAN 7 to this SSID.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi　Device Group: Default

Enable: on

* SSID: Guest_WiFi_Reyee

Band: 2.4G + 5G

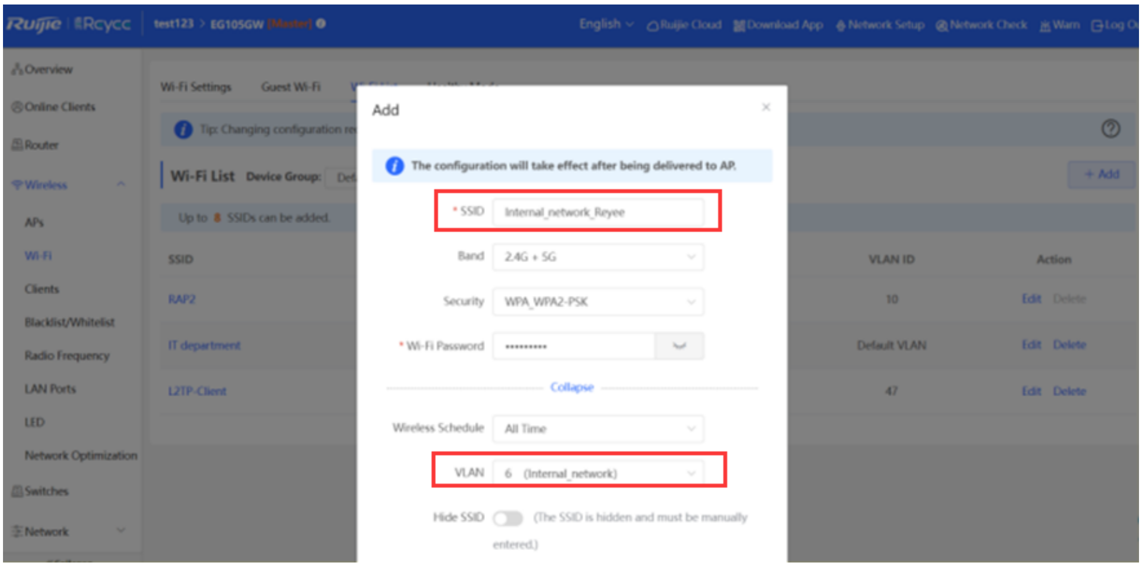
Security: WPA_WPA2-PSK

* Wi-Fi Password: •••••••••

Wireless Schedule: Never Disable

VLAN: 7 (Guest_Wi-Fi)

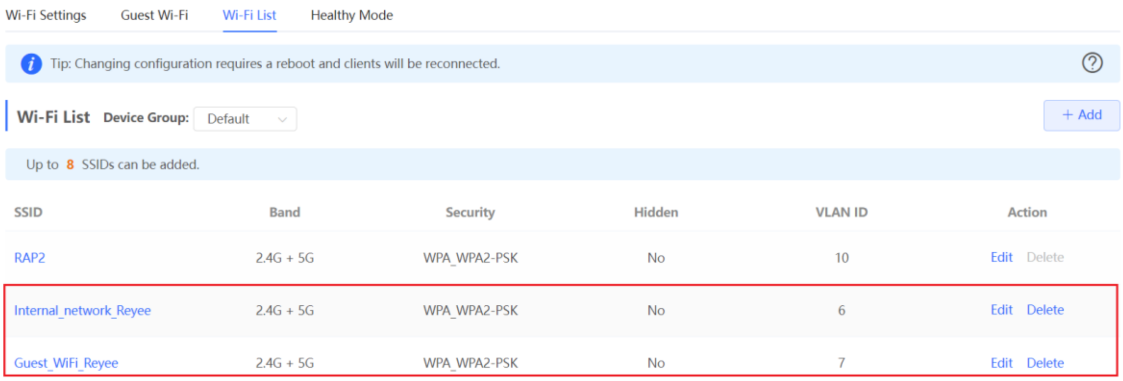
Step 4: Click **Wireless** ->**Wi-Fi** ->**Wi-Fi List** ->**Add** **c**onfigure the internal user SSID named as Internal_network_Reyee and set VLAN6 to this SSID and check the WiFi settings on the WiFi list.



Add

The configuration will take effect after being delivered to AP.

- * SSID: Internal_network_Reyee
- Band: 2.4G + 5G
- Security: WPA_WPA2-PSK
- * Wi-Fi Password: ●●●●●●●●●
- Collapse
- Wireless Schedule: All Time
- VLAN: 6 (Internal_network)
- Hide SSID: (The SSID is hidden and must be manually entered.)



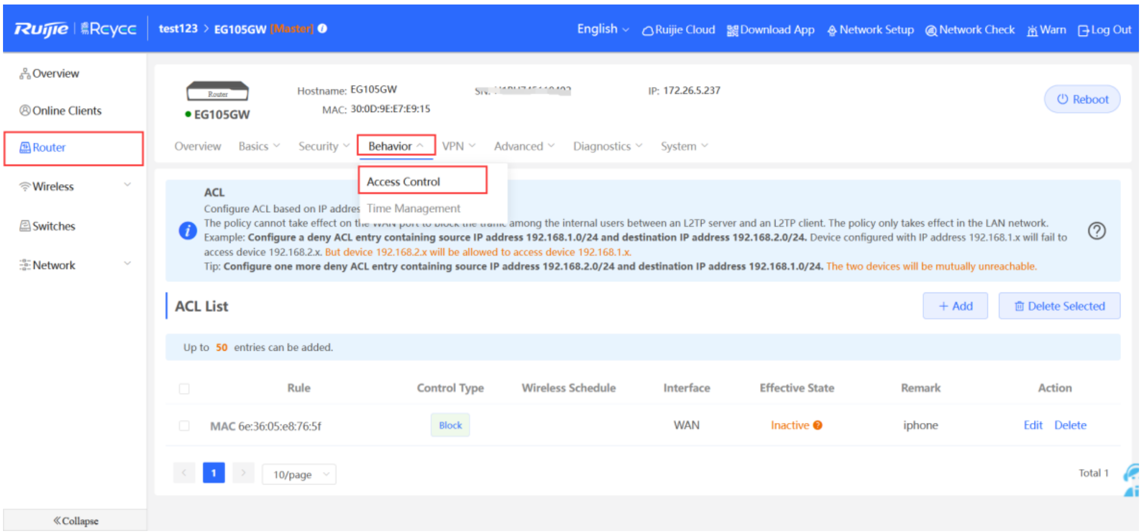
Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default + Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
RAP2	2.4G + 5G	WPA_WPA2-PSK	No	10	Edit Delete
Internal_network_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	6	Edit Delete
Guest_WiFi_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	7	Edit Delete

Step 5: Click **Router** -> **Behavior** -> **Access Control**, configure ACL to block the traffic from guest user of vlan7 network 192.168.7.0/24 to internal user of VLAN 6 192.168.6.0/24 and apply to LAN interface on EG.



Hostname: EG105GW SN: [redacted] IP: 172.26.5.237

MAC: 30:0D:9E:E7:E9:15

EG105GW

ACL

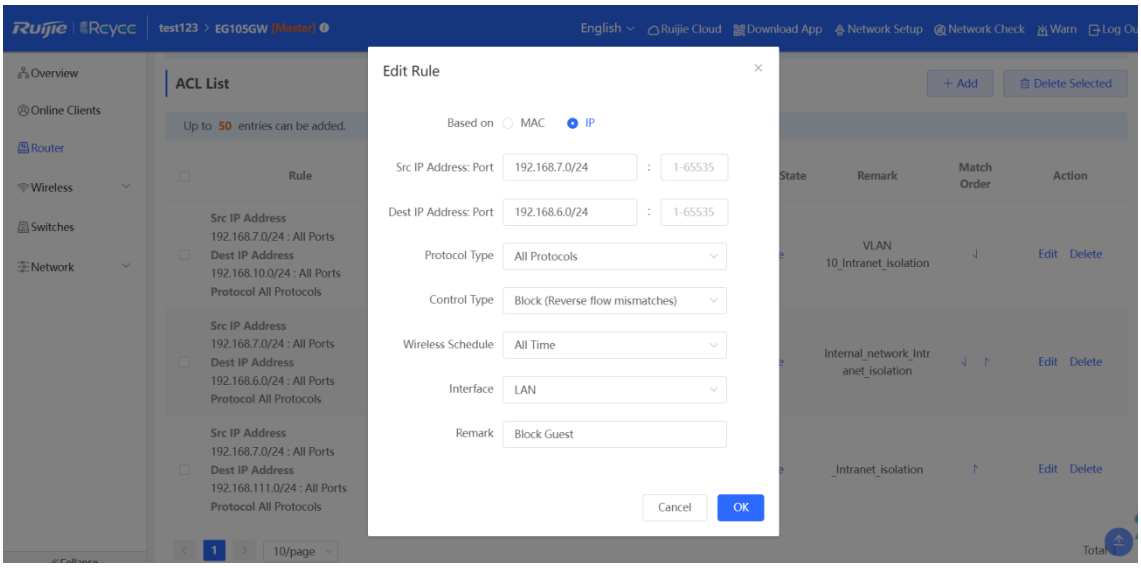
Configure ACL based on IP addres
The policy cannot take effect on the WAN port to block the traffic among the internal users between an L2TP server and an L2TP client. The policy only takes effect in the LAN network.
Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. But device 192.168.2.x will be allowed to access device 192.168.1.x.
Tip: **Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24.** The two devices will be mutually unreachable.

ACL List + Add Delete Selected

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Action
□	MAC 6e:36:05:e8:76:5f	Block		WAN	Inactive	iphone	Edit Delete

1 10/page Total 1



Edit Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.7.0/24 : 1-65535

Dest IP Address: Port 192.168.6.0/24 : 1-65535

Protocol Type All Protocols

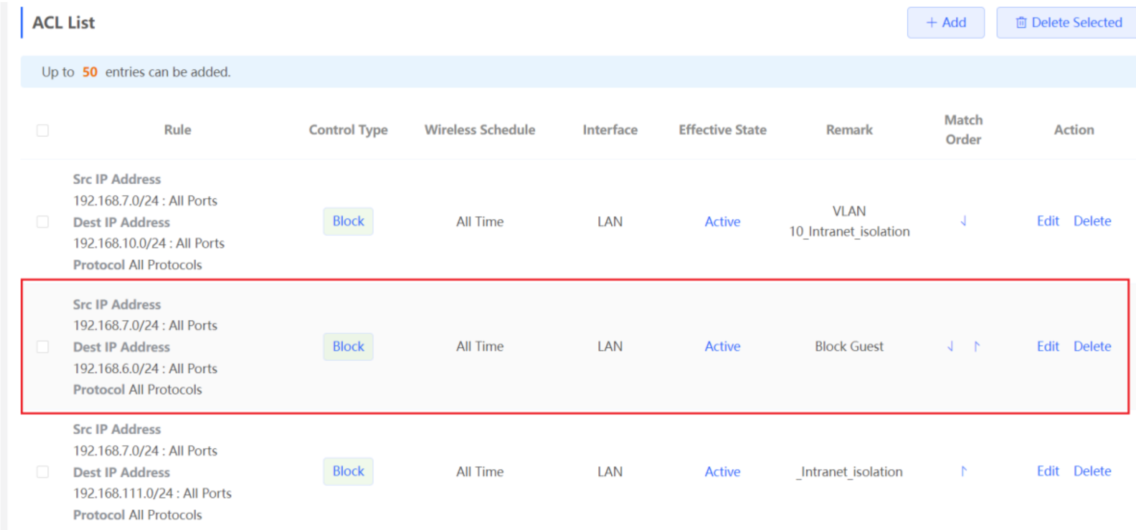
Control Type Block (Reverse flow mismatches)

Wireless Schedule All Time

Interface LAN

Remark Block Guest

Cancel OK

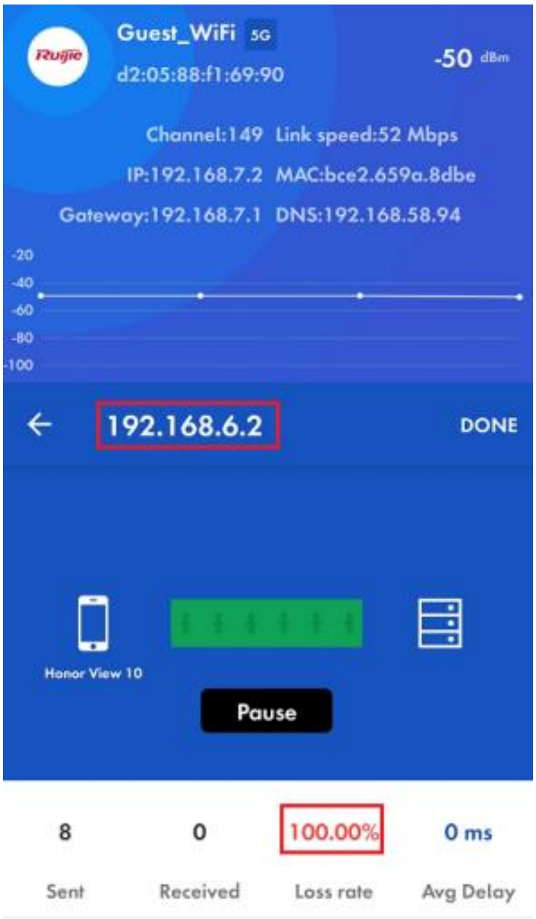


Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.10.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	VLAN 10_Intranet_isolation	↓	Edit Delete
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.6.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	Block Guest	↓ ↑	Edit Delete
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.111.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	_Intranet_isolation	↑	Edit Delete

Configuration Verification

Guest network users 192.1687.2 can’t access the internal network users 192.168.6.2.

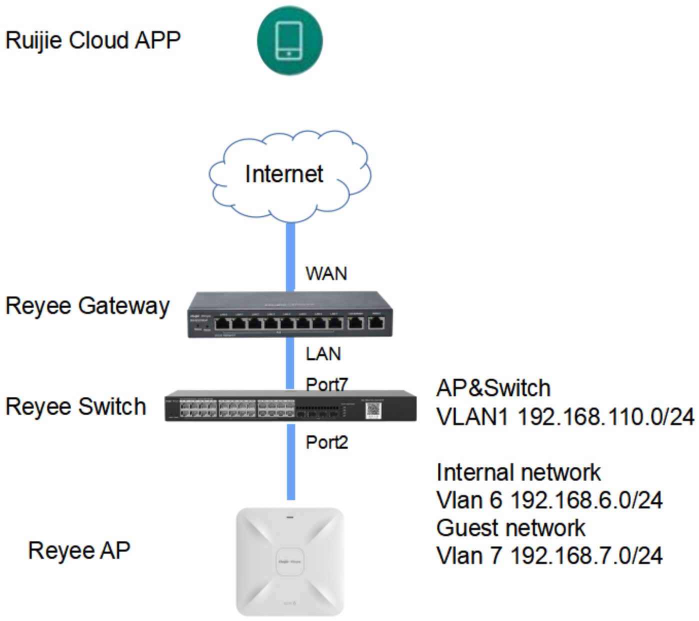


2. 5.3.3.2 Configure via Ruijie Cloud APP

Requirement

Configure Guest WiFi via Ruijie Cloud APP for Guest users in the VLAN7 network segment which cannot access the internal network in the VLAN6 network segment. Ruijie Cloud APP will deliver the corresponding configuration to device automatically..

Network Topology



Network Description：

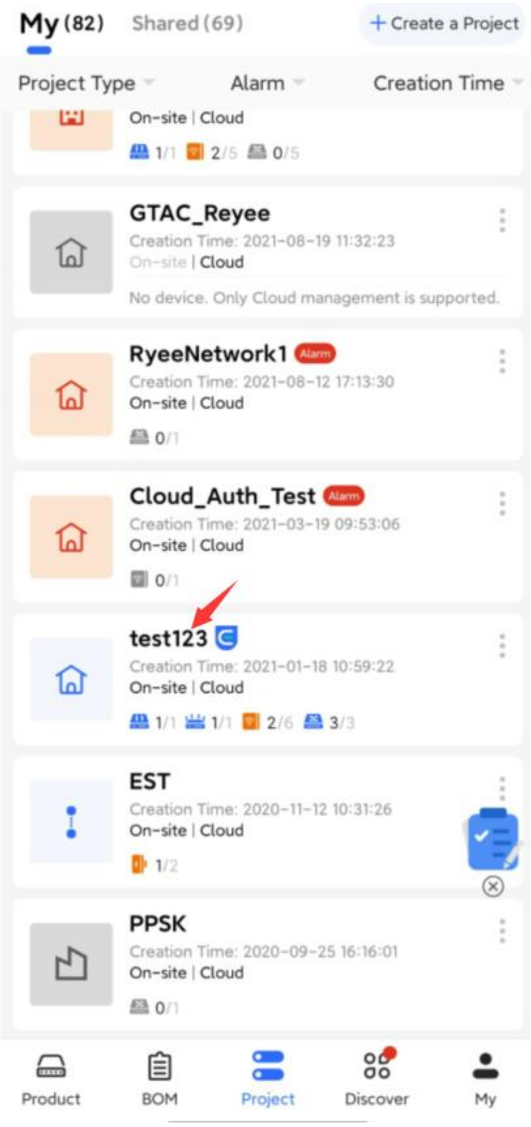
EG works as a DHCP server to assign IP addresses to users and AP & switch devices

The AP & switch devices obtain the IP address in the VLAN1 network segment for Internet access

The internal users obtain the IP address in the VLAN6 network segment for Internet access and the guest user obtain the IP address in the VLAN7 network segment for Internet access

Configuration Steps

Step1: Login to your Ruijie Cloud APP on smartphone then enter the project with Reyee gateway + RAP



My (82) Shared (69) + Create a Project

Project Type Alarm Creation Time

On-site | Cloud
1/1 2/5 0/5

GTAC_Reyee
Creation Time: 2021-08-19 11:32:23
On-site | Cloud
No device. Only Cloud management is supported.

RyeeNetwork1 Alarm
Creation Time: 2021-08-12 17:13:30
On-site | Cloud
0/1

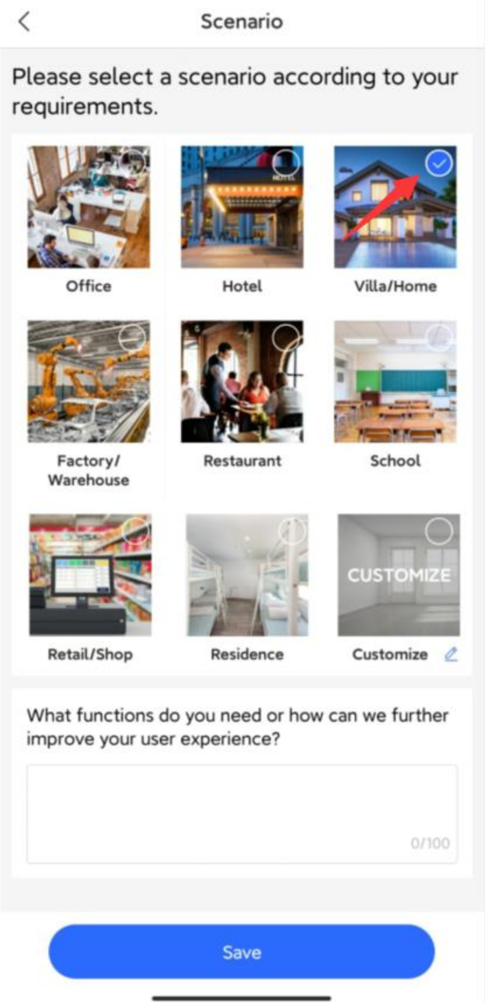
Cloud_Auth_Test Alarm
Creation Time: 2021-03-19 09:53:06
On-site | Cloud
0/1

test123
Creation Time: 2021-01-18 10:59:22
On-site | Cloud
1/1 1/1 2/6 3/3

EST
Creation Time: 2020-11-12 10:31:26
On-site | Cloud
1/2

PPSK
Creation Time: 2020-09-25 16:16:01
On-site | Cloud
0/1

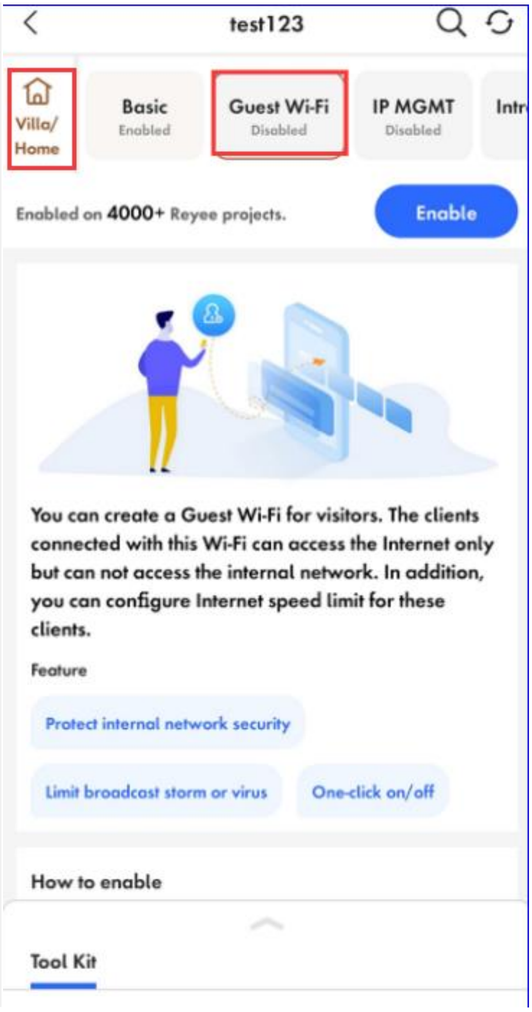
Step2: Choose Villa/Home scenario then you can see Guest Wi-Fi button.



Scenario

Please select a scenario according to your requirements.

What functions do you need or how can we further improve your user experience?

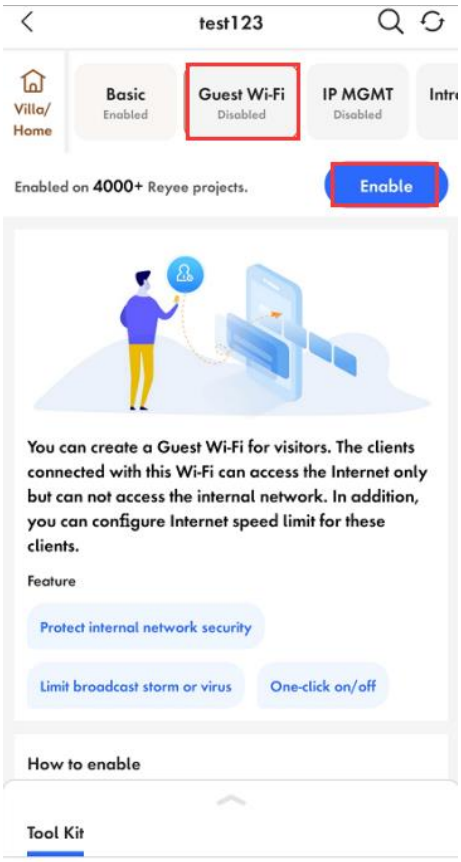


test123

Enabled on 4000+ Reyee projects.

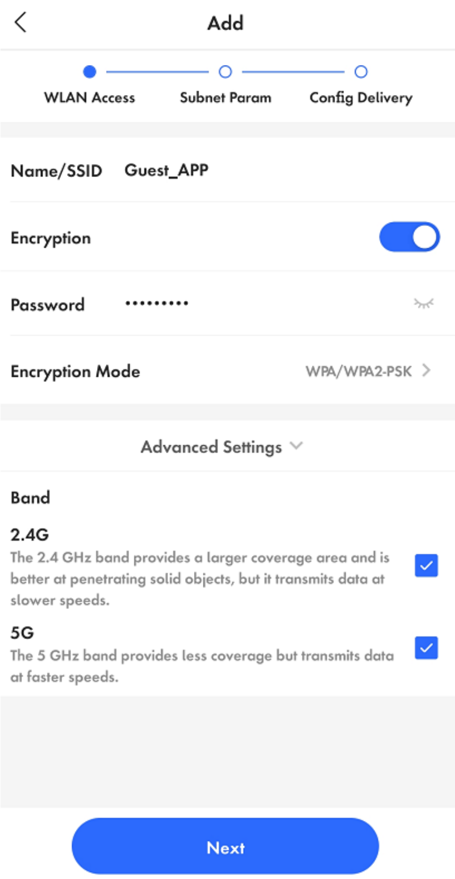
You can create a Guest Wi-Fi for visitors. The clients connected with this Wi-Fi can access the Internet only but can not access the internal network. In addition, you can configure Internet speed limit for these clients.

Step3: Select Guest Wi-Fi function and click **Enable** button.



You can create a Guest Wi-Fi for visitors. The clients connected with this Wi-Fi can access the Internet only but can not access the internal network. In addition, you can configure Internet speed limit for these clients.

Step4: Modify Guest Wi-Fi information, configure a Internal user SSID named as Guest_APP and set VLAN6 to this SSID and configure a Guest WiFi SSID named as Guest_WiFi and set VLAN7 to this SSID, then Click Save to save your configuration.



Add

● WLAN Access ○ Subnet Param ○ Config Delivery

Name/SSID Guest_APP

Encryption ●

Password •••••••••

Encryption Mode WPA/WPA2-PSK >

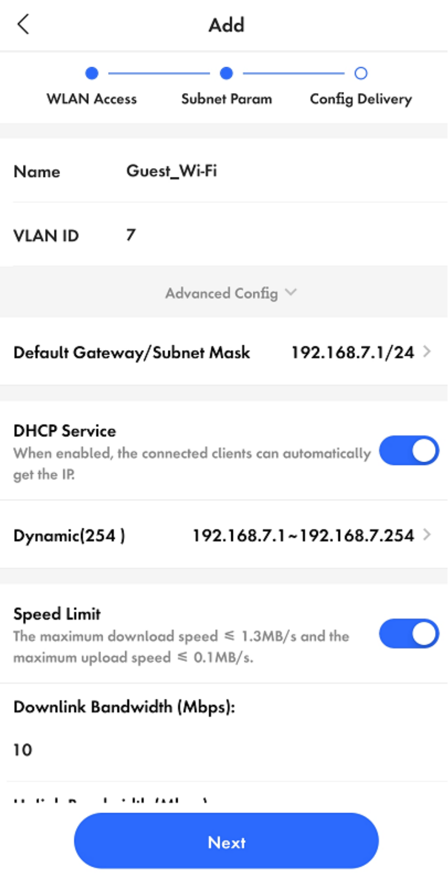
Advanced Settings ∨

Band

2.4G
The 2.4 GHz band provides a larger coverage area and is better at penetrating solid objects, but it transmits data at slower speeds. ☑

5G
The 5 GHz band provides less coverage but transmits data at faster speeds. ☑

Next



Add

● WLAN Access ● Subnet Param ○ Config Delivery

Name Guest_Wi-Fi

VLAN ID 7

Advanced Config ∨

Default Gateway/Subnet Mask 192.168.7.1/24 >

DHCP Service
When enabled, the connected clients can automatically get the IP. ●

Dynamic(254) 192.168.7.1~192.168.7.254 >

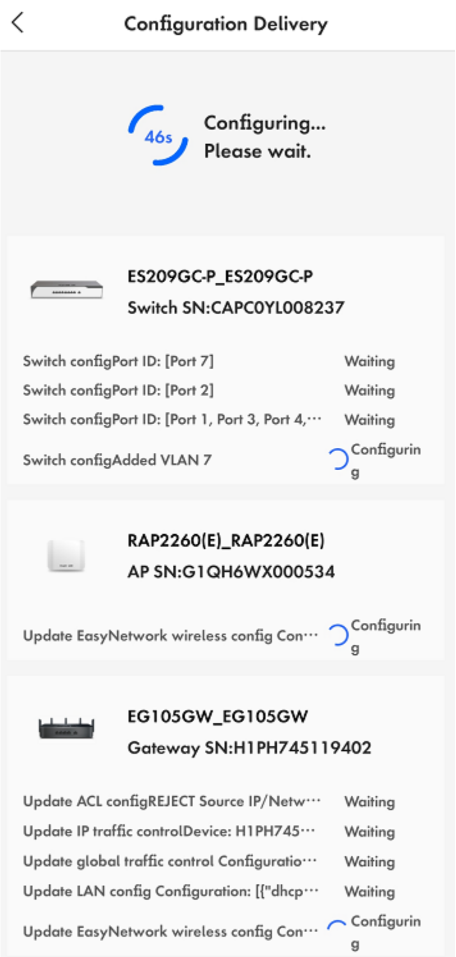
Speed Limit
The maximum download speed ≤ 1.3MB/s and the maximum upload speed ≤ 0.1MB/s. ●

Downlink Bandwidth (Mbps):

10

Next

Step4: Waiting around 1 minute for system delivering the configuration to device.



Configuration Delivery

46s Configuring...
Please wait.

ES209GC-P_ES209GC-P
Switch SN:CAPC0YL008237

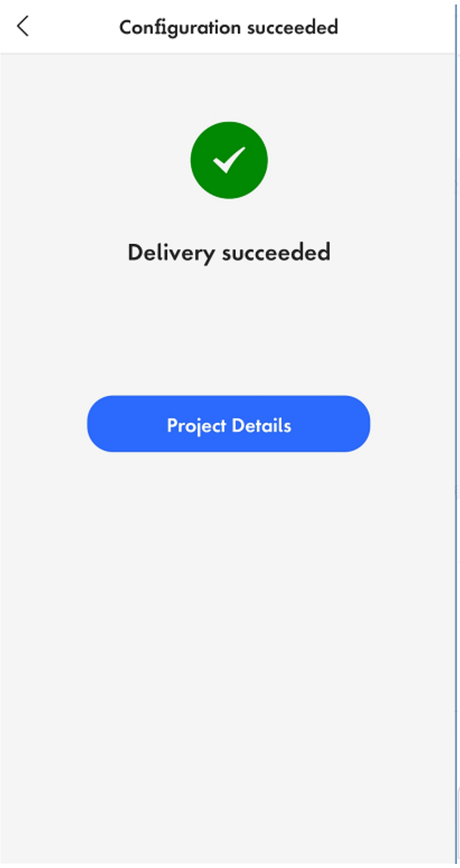
```
Switch configPort ID: [Port 7]                  Waiting
Switch configPort ID: [Port 2]                  Waiting
Switch configPort ID: [Port 1, Port 3, Port 4,…  Waiting
Switch configAdded VLAN 7                       Configurin
                                                g
```

RAP2260(E)_RAP2260(E)
AP SN:G1QH6WX000534

```
Update EasyNetwork wireless config Con…   Configurin
                                          g
```

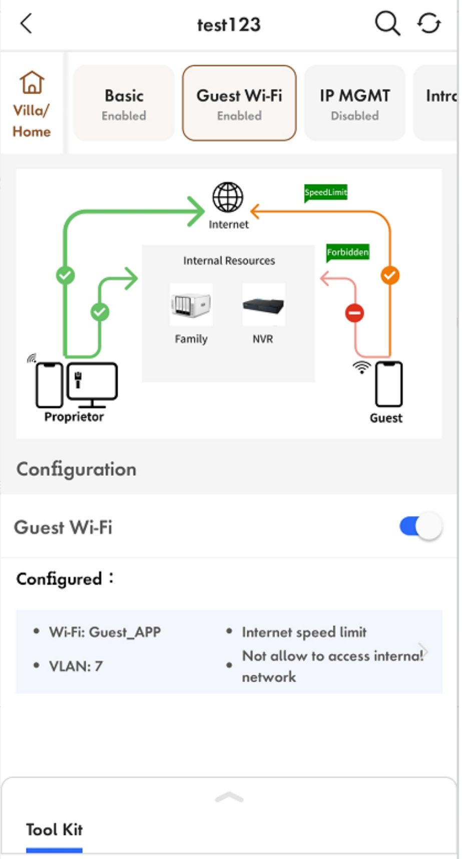
EG105GW_EG105GW
Gateway SN:H1PH745119402

```
Update ACL configREJECT Source IP/Netw…      Waiting
Update IP traffic controlDevice: H1PH745…    Waiting
Update global traffic control Configuratio…  Waiting
Update LAN config Configuration: [{"dhcp…    Waiting
Update EasyNetwork wireless config Con…      Configurin
                                             g
```



Configuration succeeded

Delivery succeeded



Configuration

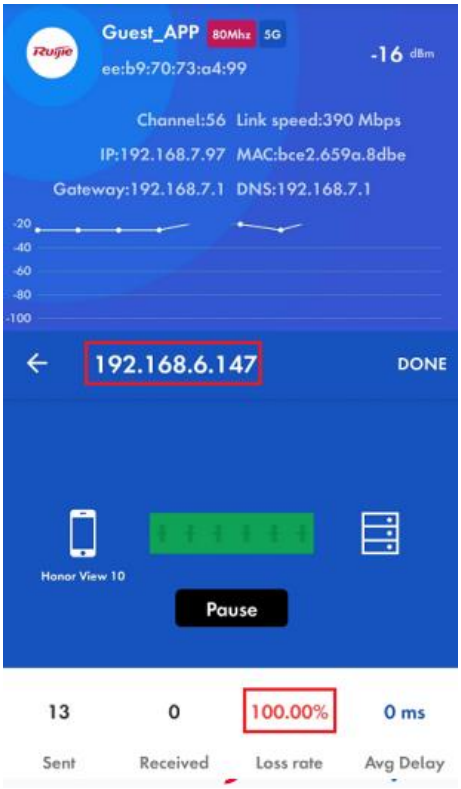
Guest Wi-Fi

Configured：

- Wi-Fi: Guest_APP
- VLAN: 7
- Internet speed limit
- Not allow to access internal network

Configuration Verification

The guest user 192.168.7.97 can’t be able to access the internal user 192.168.6.147.



Guest_APP 80Mhz 5G

ee:b9:70:73:a4:99

-16 dBm

Channel:56 Link speed:390 Mbps

IP:192.168.7.97 MAC:bce2.659a.8dbe

Gateway:192.168.7.1 DNS:192.168.7.1

192.168.6.147 DONE

13	0	100.00%	0 ms
Sent	Received	Loss rate	Avg Delay

20.4 Reyee SON—Self-Organizing Network

Self-organizing network feature, which breaks through the product limitations and realizes auto-discovery, auto-networking and auto-configuration between routers, switches, and wireless APs without the need for controllers or internet access. With the mobile APP, users can quickly complete the device deployment and configuration, remote management, operation and maintenance of the entire networks, which greatly reduces the investment of equipment cost, labor cost and time cost in the process of wireless network construction.

20.4.1 The principle of Reyee SON

1. 5.4.1.1 Network ID

Every device has its own network ID.

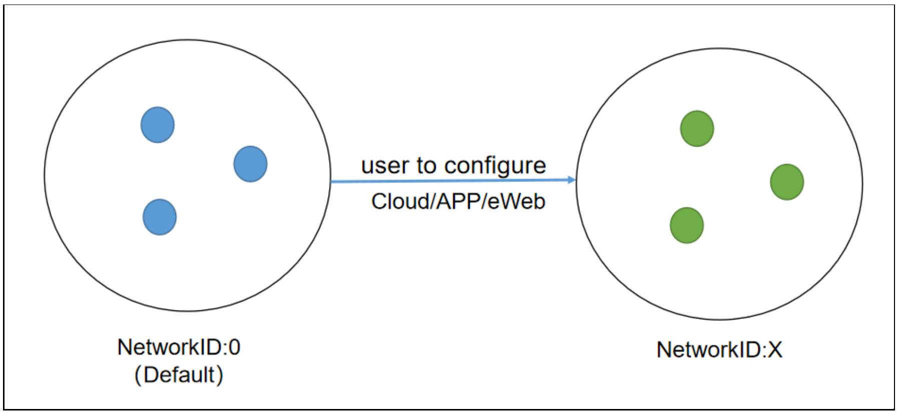
Only devices with the same networkID can be added to a network.

Devices with different networkID should be merged before added to the same network.

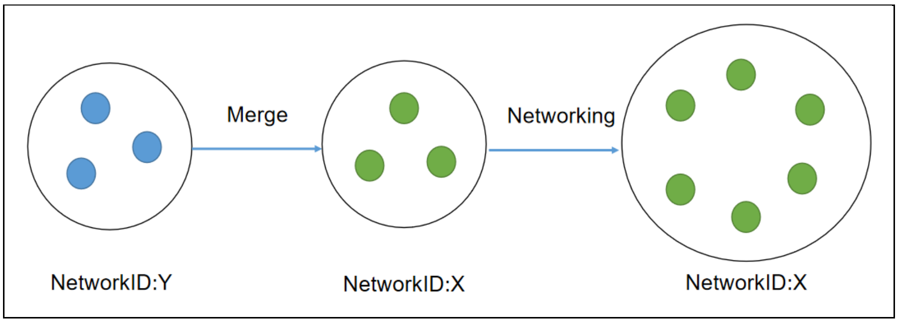
The network ID is 0 by default.

After the device is configured, it will have a new network ID(networkid is non-zero).

After configure:



Merge:



2. 5.4.1.2 Protocol

Easydisc

Responsible for neighbor discovery, master election, and notification of master changes.

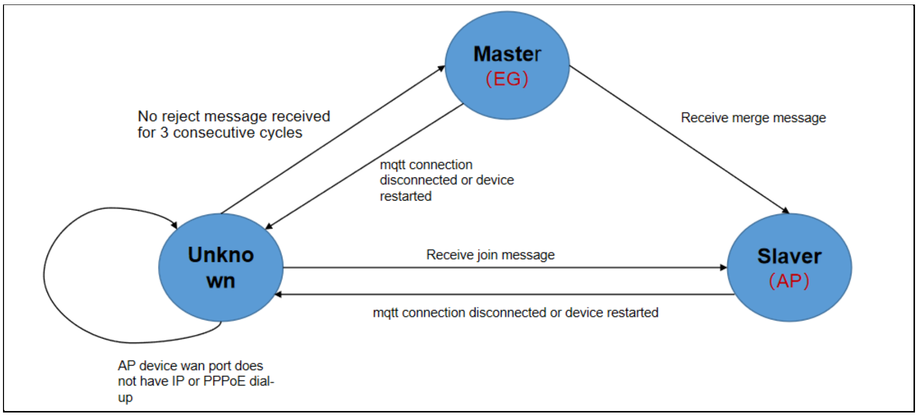
Easydisc is a proprietary protocol and uses UDP port numbers 43561 and 43562 for communication.

MQTT

Responsible for the collection of networking equipment information, the collection of STA information, and the synchronization of configuration information.

MQTT is a standard protocol and uses TCP port number 1883 for communication.

3. 5.4.1.3 Easydisc – Role



4. 5.4.1.4 Easydisc- packet

Packet type:

Declare: broadcast; in the Initial state, broadcast declares message; send its own priority and other related information.

Reject: unicast; when receiving the decade message, according to the election priority, if its own priority is higher, it will reply reject.

Join: broadcast; sent by the master, when other initial states receive the message, they will connect to the master according to the master information in it.

Conflict: unicast; the master sends a conflict message when it receives a join message from another master and cannot be resolved according to the conflict handling algorithm.

Merge: unicast; the master sends a merge message when it receives a join message from other masters and can merge the other party's network according to the conflict handling algorithm.

Hello: broadcast; all devices start broadcasting hello packets after the role status is confirmed for neighbor discovery.

5. 5.4.1.5 Master election roles

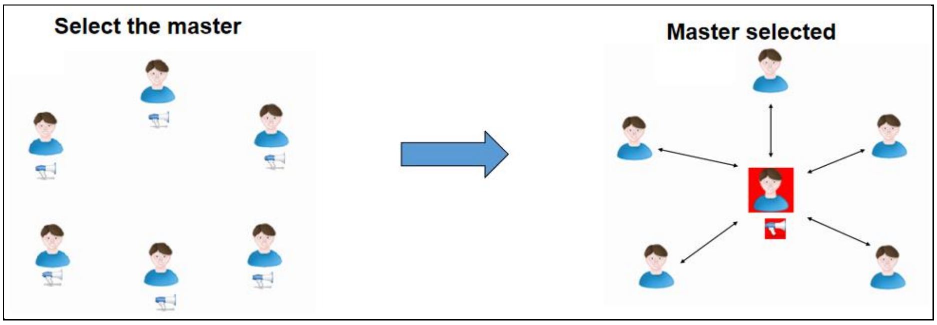
Priority:

(1) EG > AP > SW

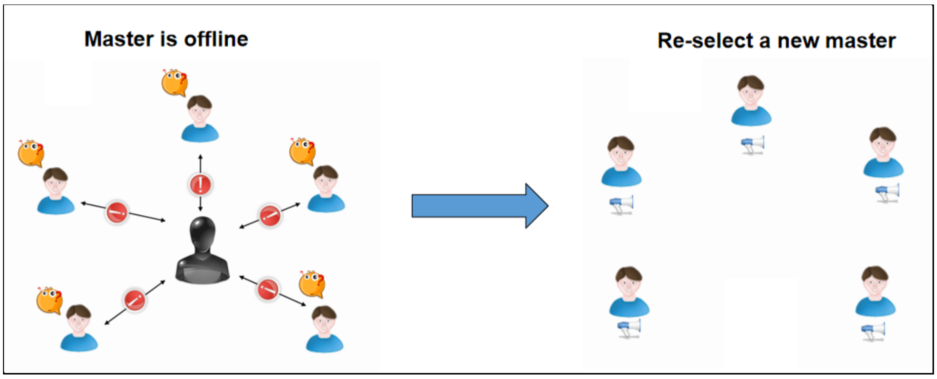
(2) Device model: device CPU/Memory/other(AP radio number)

(3) When the priorities are the same, the larger MAC address will be the master.

Select the Master:



Re-select the Master:



6. 5.4.1.6 Master preemption mechanism

If a device with a higher priority joins a network, the master device will change. The new device will send a merge packet to the master device.

1.For AP networking, after the master is selected, if a new EG is added, EG will become the master.

Delay time: 7-8s

2.For AP networking, after the master is selected, if a new AP with a higher priority is added, the preempt is delayed.

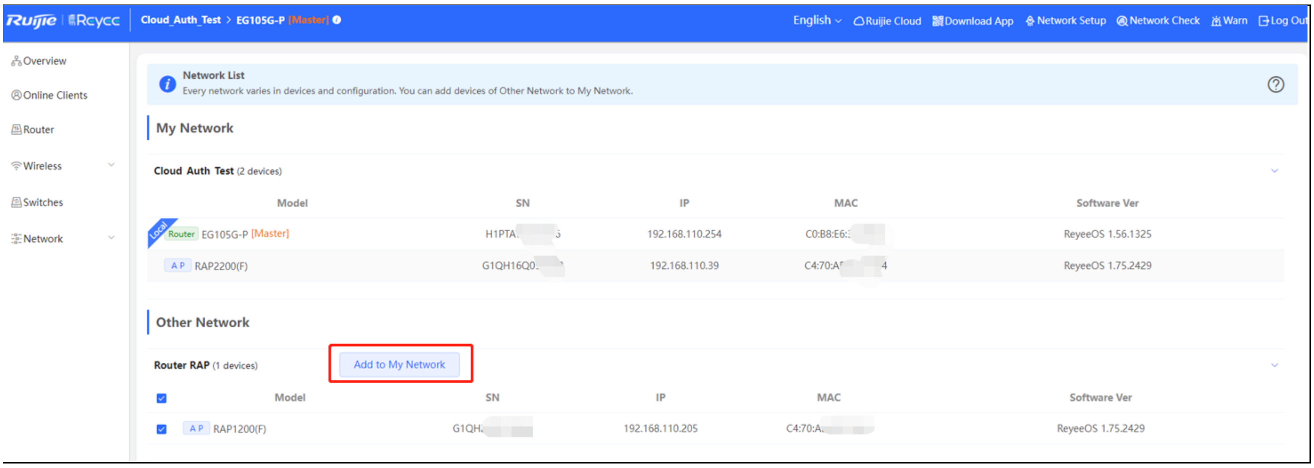
Delay time: preemption starts after the master is powered on for 36 hours and the new device is powered on for 5 minutes; otherwise, preemption starts after the new device is powered on for 30 minutes.

For AP+SW networking, after the master is selected, if a new EG is added, EG will become the master.

20.4.2 The configuration of Reyee SON

1. 5.4.1.1 Neighbor Discovery

Add devices of other networks to **My Network**.



Network List
Every network varies in devices and configuration. You can add devices of Other Network to My Network.

My Network

Cloud_Auth_Test (2 devices)

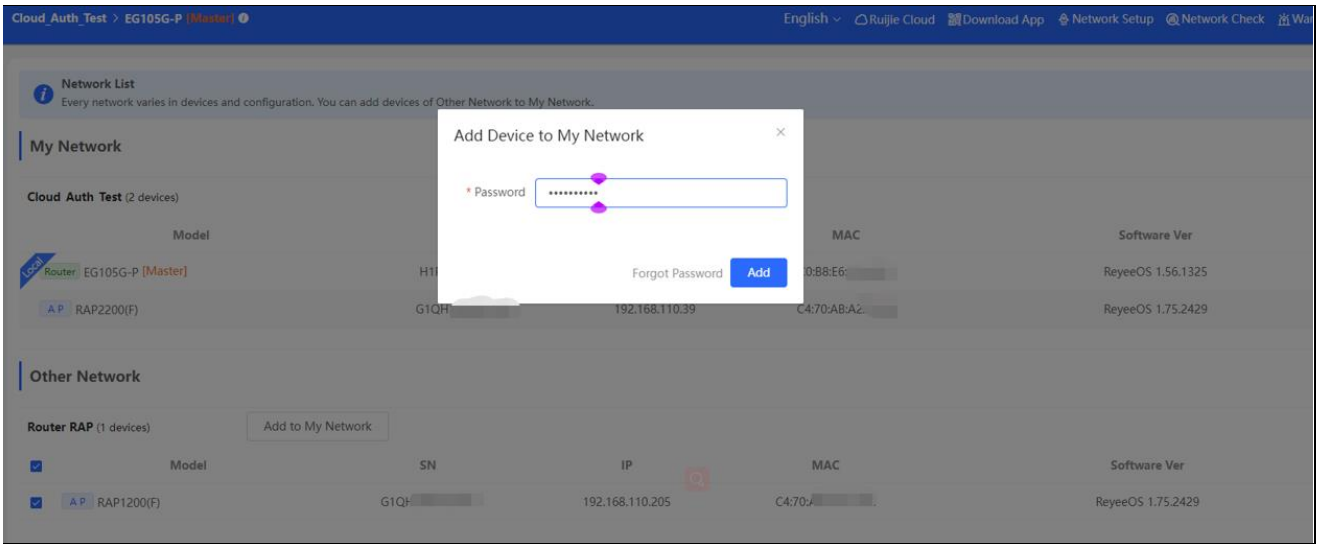
Model	SN	IP	MAC	Software Ver
Router EG105G-P [Master]	H1PTA[redacted]5	192.168.110.254	C0:B8:E6:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1QH16Q0[redacted]	192.168.110.39	C4:70:A[redacted]4	ReyeeOS 1.75.2429

Other Network

Router RAP (1 devices)

☑	Model	SN	IP	MAC	Software Ver
☑	AP RAP1200(F)	G1QH[redacted]	192.168.110.205	C4:70:A[redacted]	ReyeeOS 1.75.2429

Enter the password of device.



Network List
Every network varies in devices and configuration. You can add devices of Other Network to My Network.

Add Device to My Network

* Password ••••••••••

My Network

Cloud_Auth_Test (2 devices)

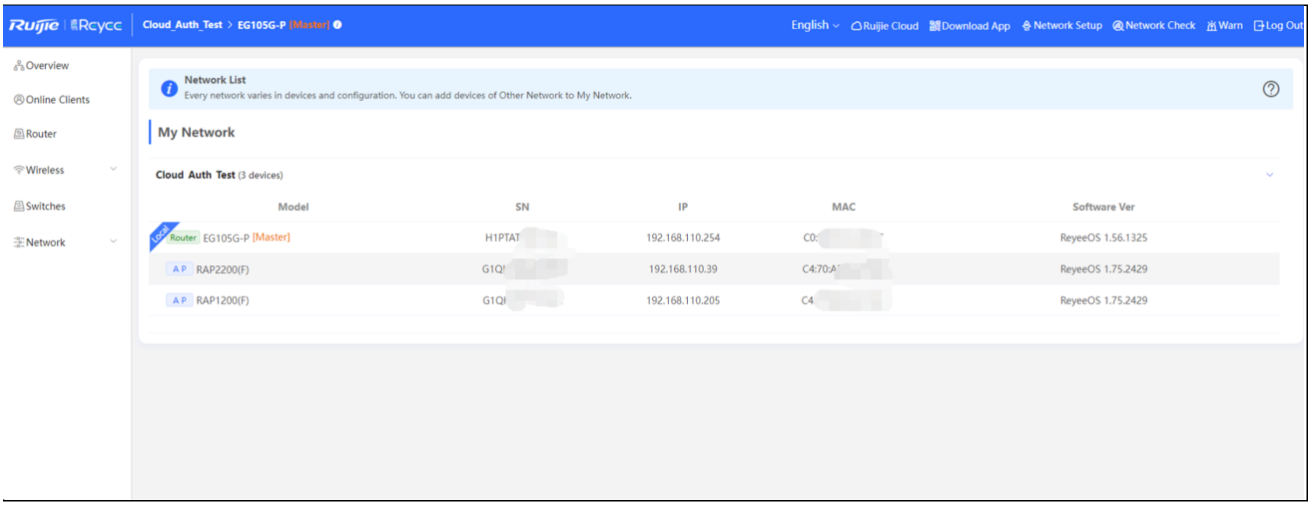
Model	SN	IP	MAC	Software Ver
Router EG105G-P [Master]	H1		0:B8:E6:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1QH[redacted]	192.168.110.39	C4:70:AB:A2[redacted]	ReyeeOS 1.75.2429

Other Network

Router RAP (1 devices)

☑	Model	SN	IP	MAC	Software Ver
☑	AP RAP1200(F)	G1QH[redacted]	192.168.110.205	C4:70:A[redacted]	ReyeeOS 1.75.2429

Device is added to the network.



Network List

Every network varies in devices and configuration. You can add devices of Other Network to My Network.

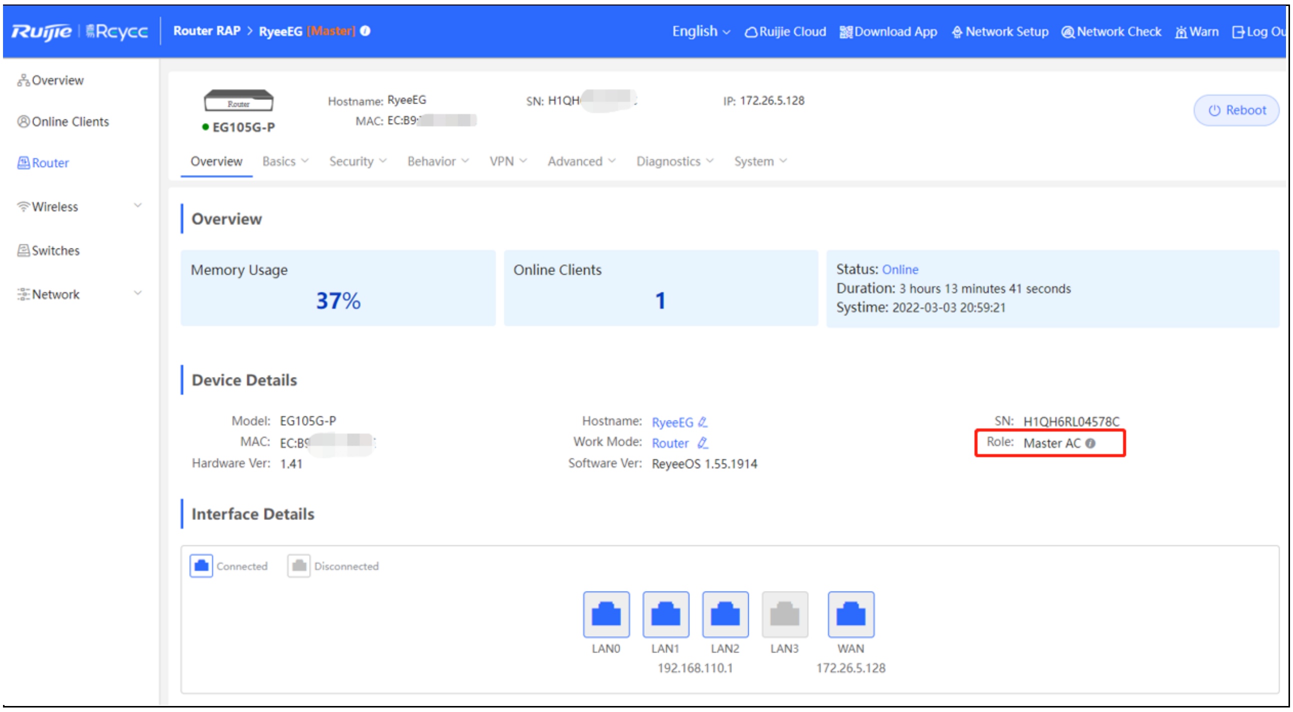
My Network

Cloud Auth Test (3 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105G-P [Master]	H1PTAT[redacted]	192.168.110.254	C0:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1Q[redacted]	192.168.110.39	C4:70:A[redacted]	ReyeeOS 1.75.2429
AP RAP1200(F)	G1Q[redacted]	192.168.110.205	C4[redacted]	ReyeeOS 1.75.2429

2. 5.4.1.2 Device networking role

Master:



● EG105G-P

Hostname: RyeeEG

MAC: EC:B9:[redacted]

SN: H1QH[redacted]

IP: 172.26.5.128

Overview

Memory Usage 37%

Online Clients 1

Status: Online

Duration: 3 hours 13 minutes 41 seconds

Systime: 2022-03-03 20:59:21

Device Details

Model: EG105G-P

MAC: EC:B9[redacted]

Hardware Ver: 1.41

Hostname: RyeeEG

Work Mode: Router

Software Ver: RyeeOS 1.55.1914

SN: H1QH6RL04578C

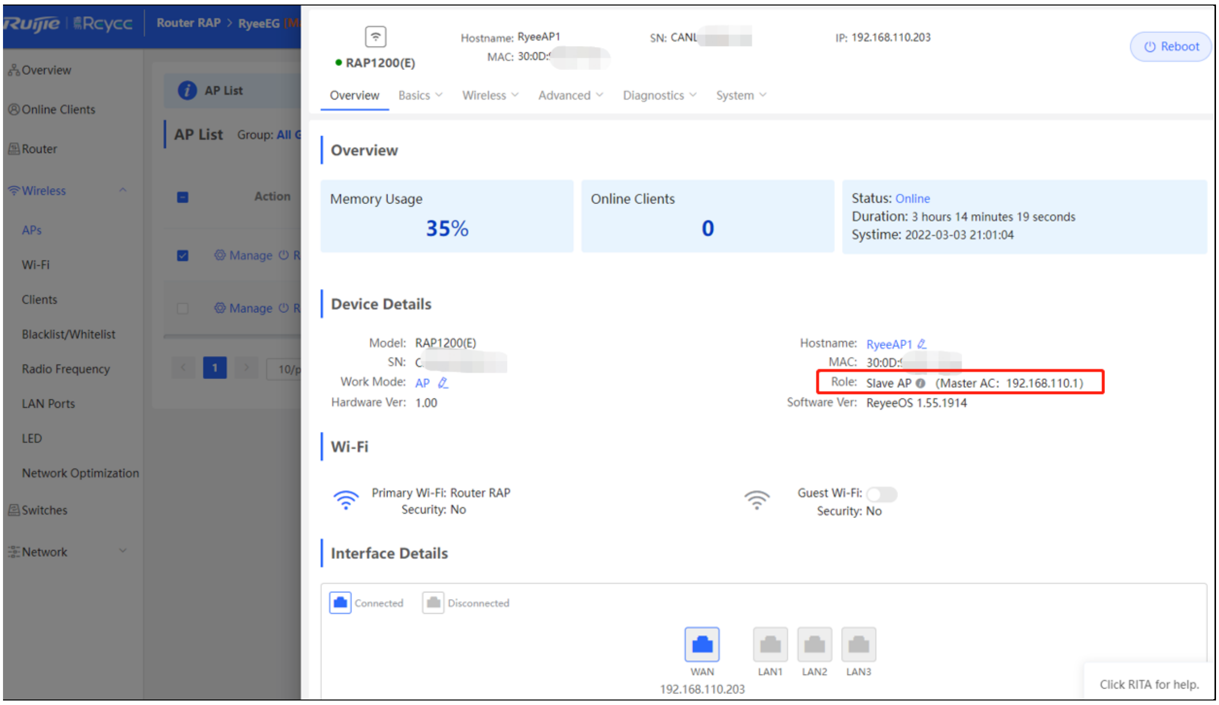
Role: Master AC

Interface Details

192.168.110.1

172.26.5.128

Slave:



RAP1200(E)

Hostname: RyeeAP1
MAC: 30:0D:[redacted]
SN: CANL[redacted]
IP: 192.168.110.203

Overview

Memory Usage 35%

Online Clients 0

Status: Online
Duration: 3 hours 14 minutes 19 seconds
Systime: 2022-03-03 21:01:04

Device Details

Model: RAP1200(E)
SN: C[redacted]
Work Mode: AP
Hardware Ver: 1.00

Hostname: RyeeAP1
MAC: 30:0D:[redacted]
Role: Slave AP (Master AC: 192.168.110.1)
Software Ver: ReyeeOS 1.55.1914

Wi-Fi

Primary Wi-Fi: Router RAP
Security: No

Guest Wi-Fi:
Security: No

Interface Details

WAN 192.168.110.203

20.4.3 The troubleshooting of SON

Fault symptom

Network self-organization Fail

Cause

There are multiple masters, and more than 1 @Ruijie-mxxx SSID could be seen.

Layer fails to broadcast.

Solution

Check whether the devices are connected with same network and merge all the devices to the same network.

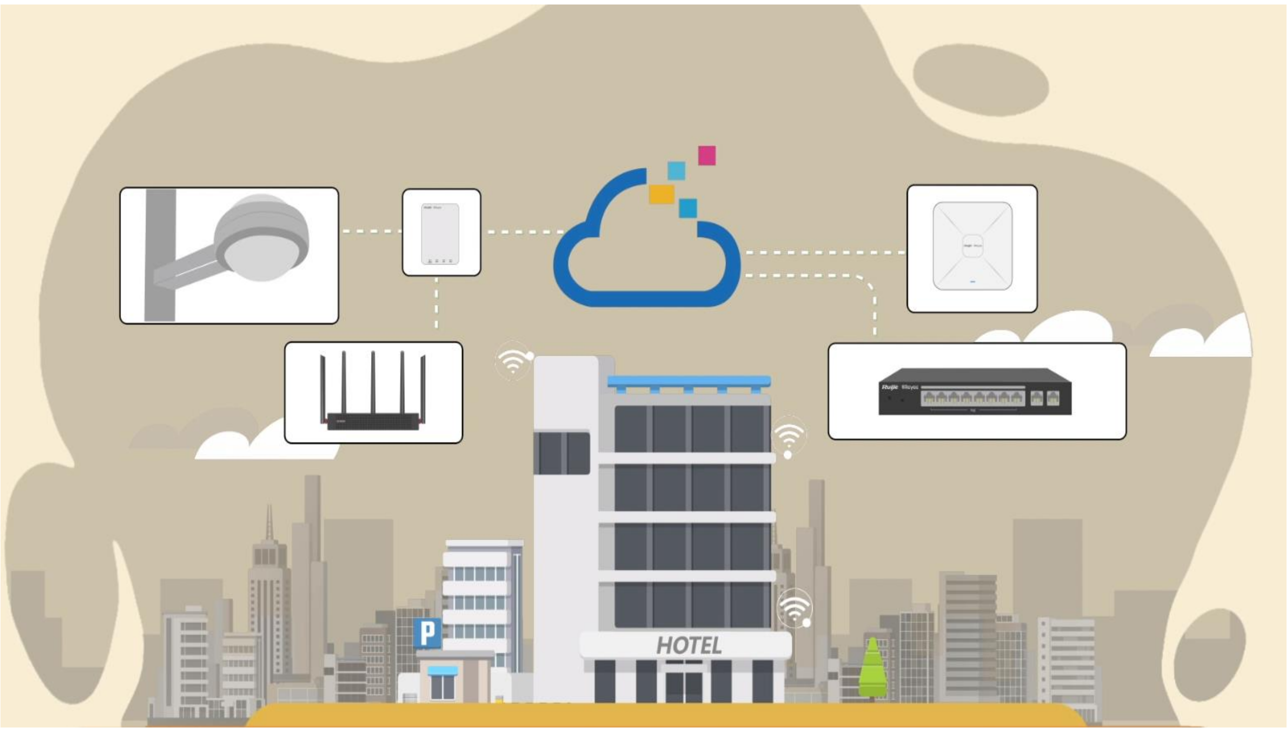
Check whether there are have some configurations like VLAN and port isolation.

Check whether the SON is disabled.

20.5 Reyee Economic Hotel Network Solution

20.5.1 Application Scenario

Reyee economic hotel network solution provides an affordable 5-star Wi-Fi for clients. It can operate concurrently at 2.4GHz and 5GHz, providing high-speed wireless access of 574Mbps at 2.4GHz, 1201Mbps at 5GHz and up to 1775Mbps per AP. The wall AP provides a LAN port at the front to facilitate the expansion of IPTV, IP phone, etc.



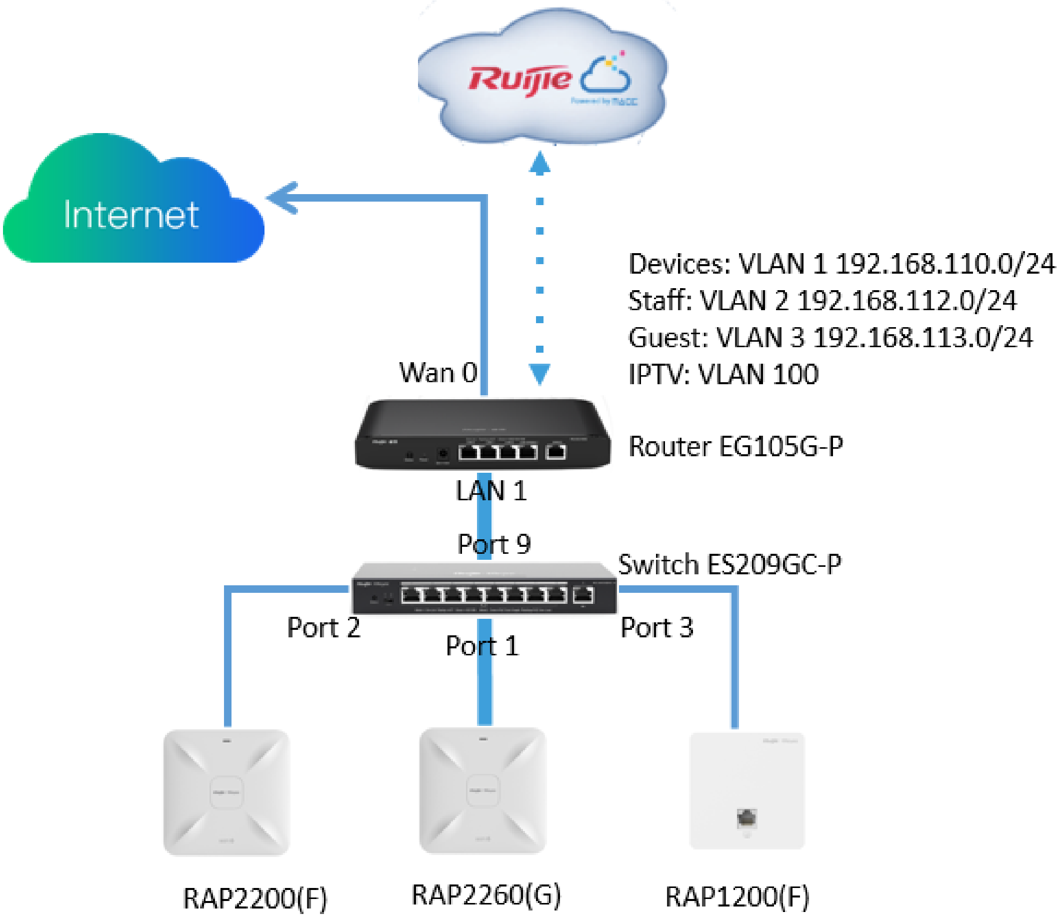
20.5.2 Configuration Case

Requirement

1. Wireless network for Hotel, guests need to do voucher authentication before accessing internet and can’t access internal network of hotel.

2. Providing wired connection for IPTV.

Network Topology



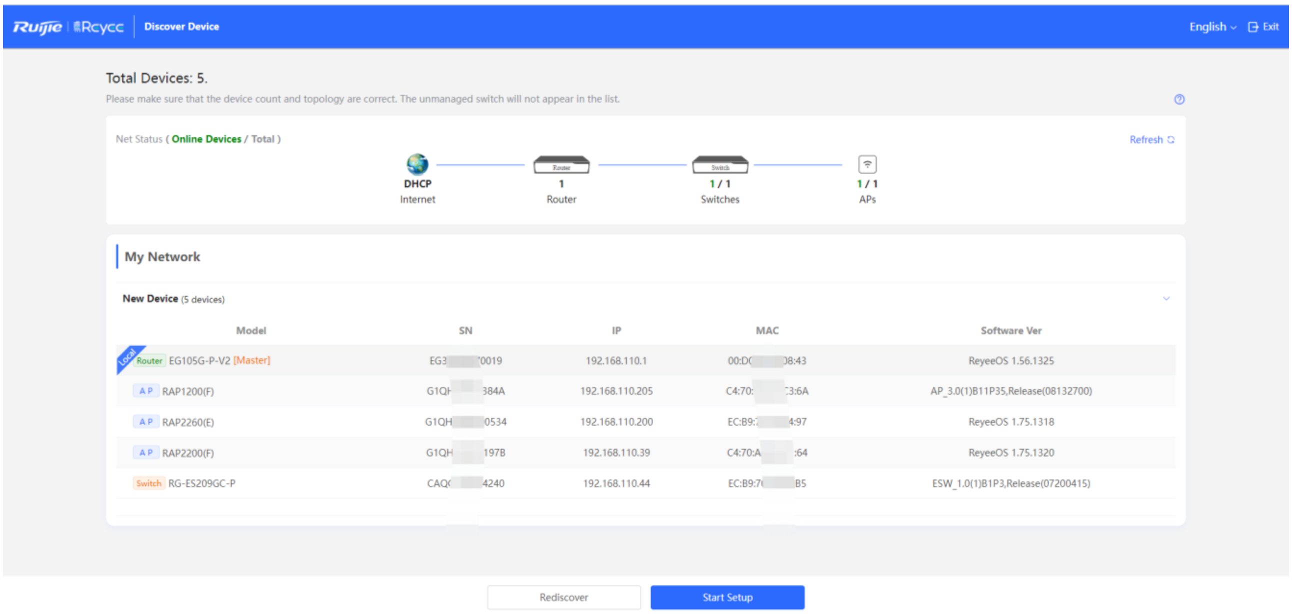
Devices List

Type	Model	Function
Gateway	EG105G-P	1.Connect Internet and work as DHCP server for downlink devices and clients; 2.Manage AP and Switch Devices locally; 3.Support Cloud voucher authentication with Ruijie Cloud;
Switch	ES209GC-P	Provide wired and POE connection.
Wall AP	RAP1200(F)	1.Provide wireless connection for room. 2.Provide wired connection for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provide wireless connection for hall and corridor.

Configuration Steps

Step1: Power on and connect the device refer to the topology.

Step2: Access Gateway by default IP 192.168.110.1, refer the **Start Setup** step to configure the basic network settings.



Total Devices: 5.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

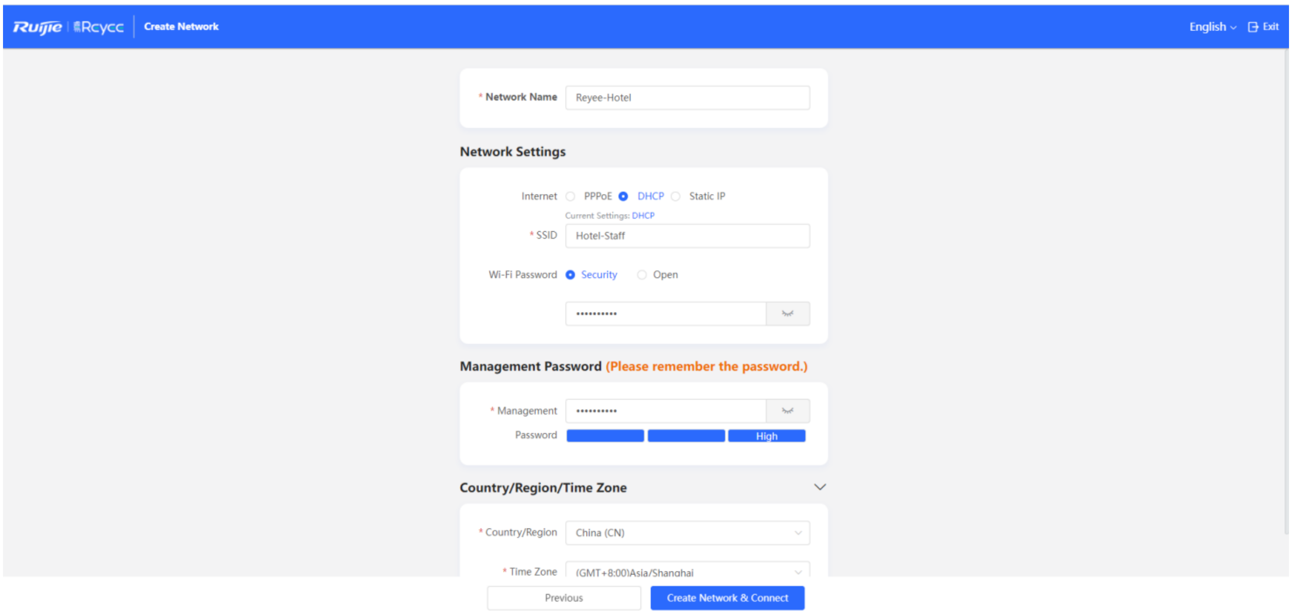
Net Status (Online Devices / Total) Refresh

My Network

New Device (5 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105G-P-V2 [Master]	EG3[redacted]0019	192.168.110.1	00:DC[redacted]08:43	ReyeeOS 1.56.1325
AP RAP1200(F)	G1QH[redacted]384A	192.168.110.205	C4:70:[redacted]3:6A	AP_3.0(1)B11P35,Release(08132700)
AP RAP2260(E)	G1QH[redacted]0534	192.168.110.200	EC:B9:[redacted]4:97	ReyeeOS 1.75.1318
AP RAP2200(F)	G1QH[redacted]197B	192.168.110.39	C4:70:A[redacted]:64	ReyeeOS 1.75.1320
Switch RG-ES209GC-P	CAQ[redacted]4240	192.168.110.44	EC:B9:7[redacted]B5	ESW_1.0(1)B1P3,Release(07200415)

Set the **Network Name**, **Network Settings, SSID** for Staffs and the set the **Management Password.**



* Network Name: Reyee-Hotel

Network Settings

Internet ○ PPPoE ● DHCP ○ Static IP

Current Settings: DHCP

* SSID: Hotel-Staff

Wi-Fi Password ● Security ○ Open

••••••••••

Management Password (Please remember the password.)

* Management Password: ••••••••••

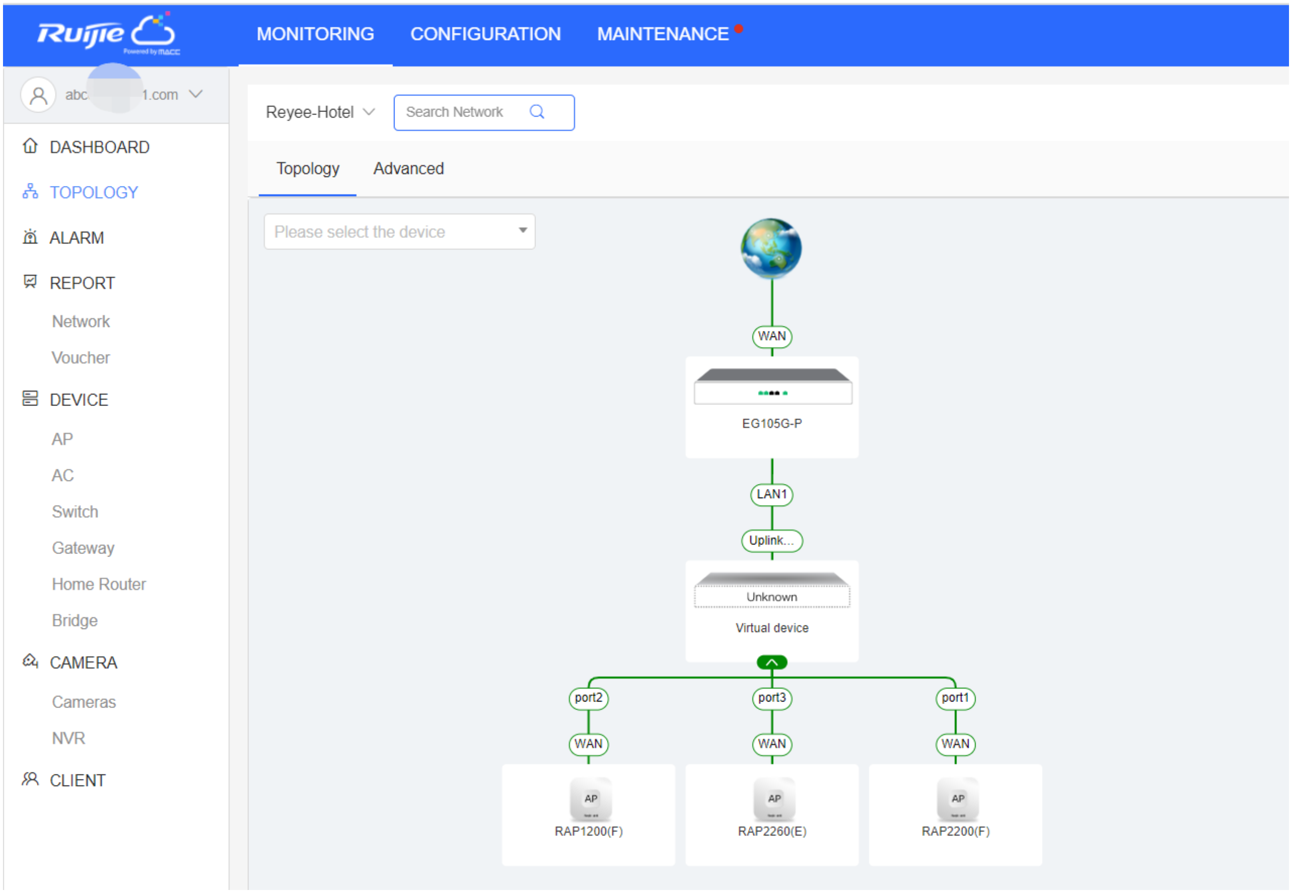
High

Country/Region/Time Zone

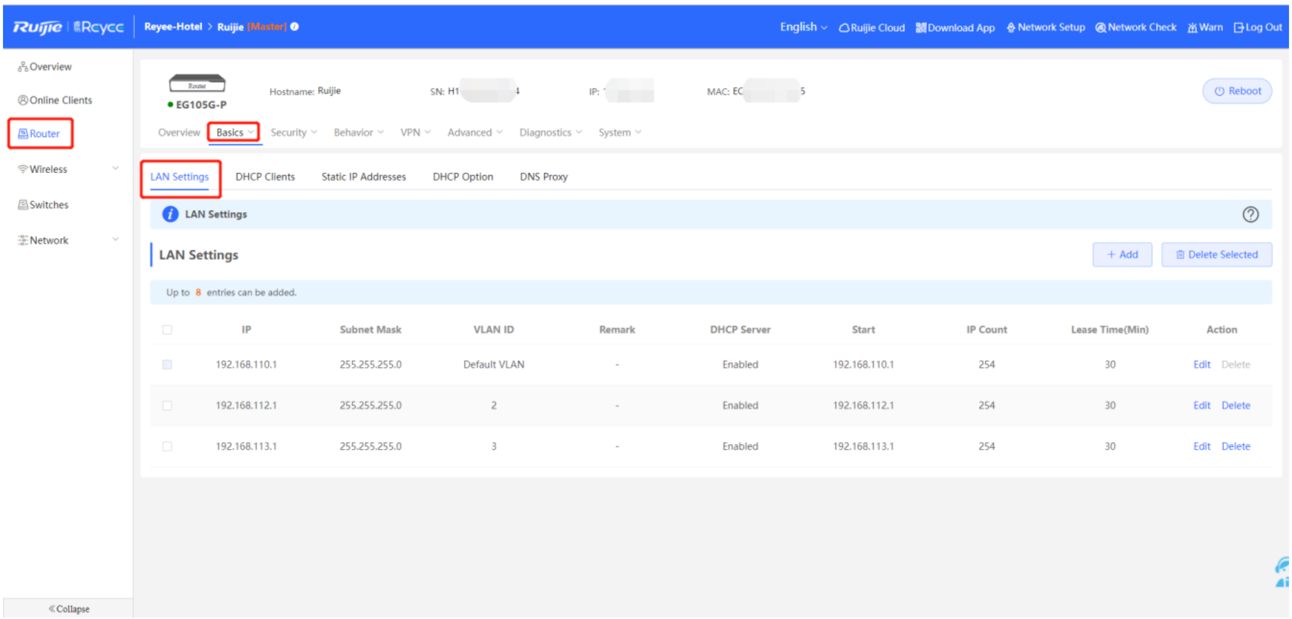
* Country/Region: China (CN)

* Time Zone: (GMT+8:00)Asia/Shanghai

Click **Create Network & Connect** to active configuration and add the devices to Cloud.



Step2: Click **Router->Basic->LAN** to create VLAN 2 and VLAN 3 for Staff and Guest.



● EG105G-P

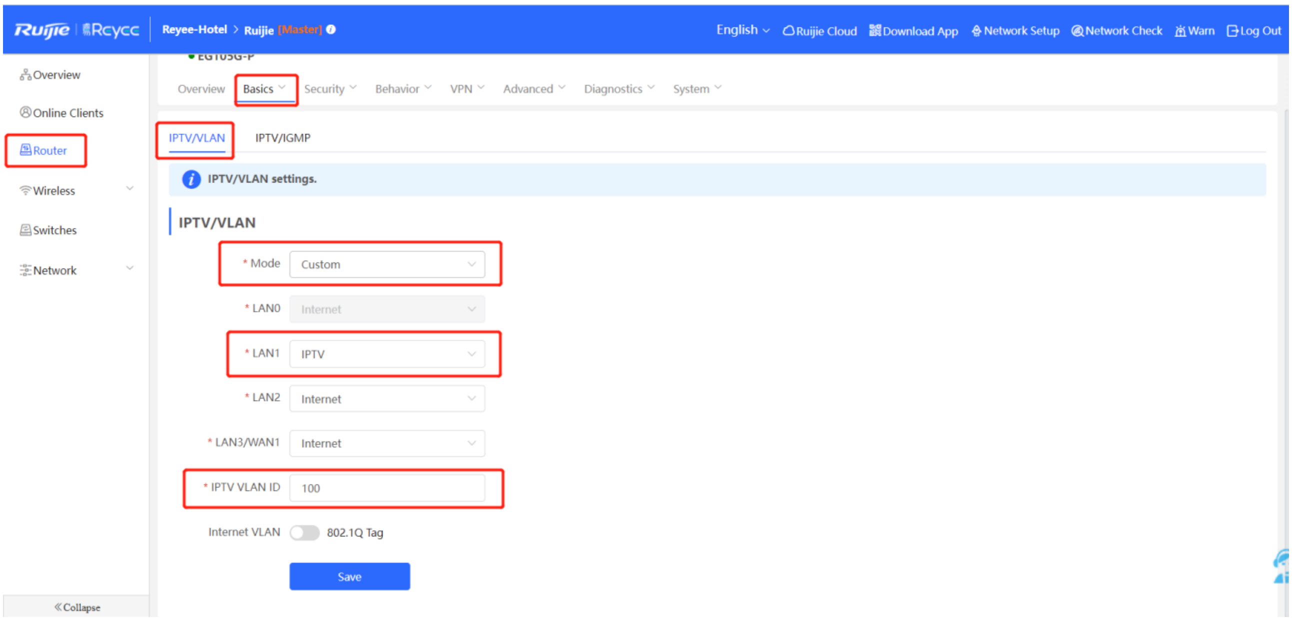
Hostname: Ruijie SN: [redacted] IP: [redacted] MAC: [redacted]

LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
□	192.168.112.1	255.255.255.0	2	-	Enabled	192.168.112.1	254	30	Edit Delete
□	192.168.113.1	255.255.255.0	3	-	Enabled	192.168.113.1	254	30	Edit Delete

Step3: Click **Router->Basic->IPTV** to set IPTV settings get from ISP. For example, the IPTV VLAN is 100, you can do as below:.



IPTV/VLAN settings.

IPTV/VLAN

* Mode: Custom

* LAN0: Internet

* LAN1: IPTV

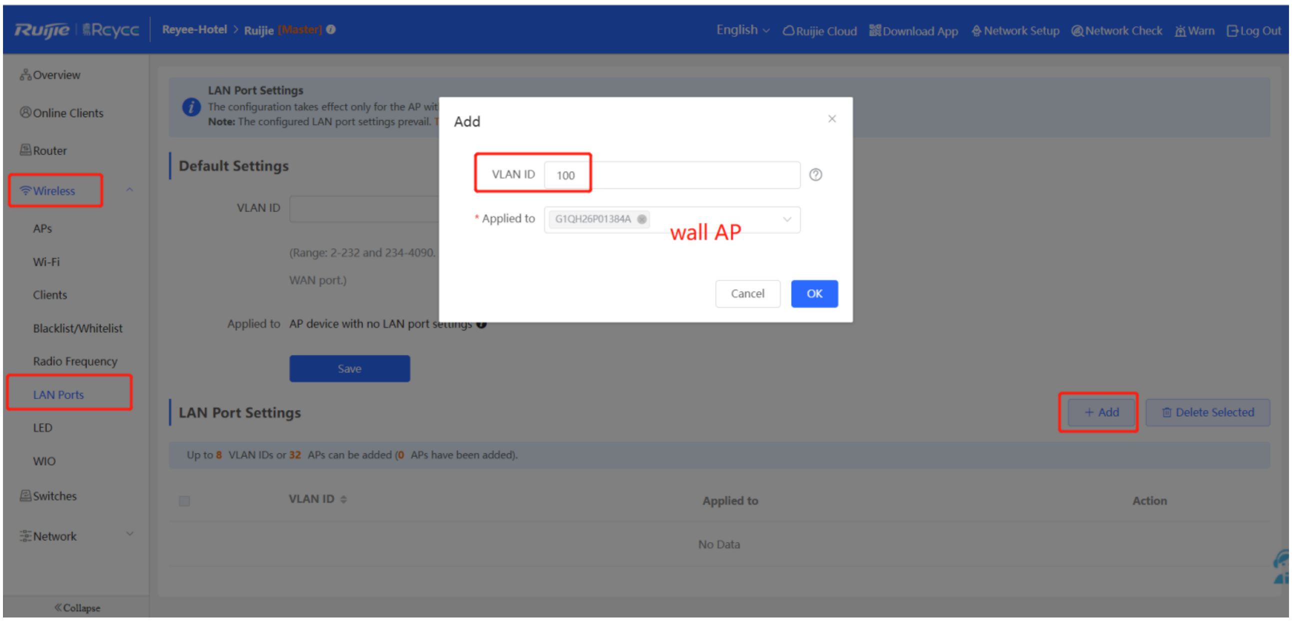
* LAN2: Internet

* LAN3/WAN1: Internet

* IPTV VLAN ID: 100

Internet VLAN: 802.1Q Tag

Step4: Click **Wireless->LAN Ports->Add** to configure VLAN 100 for IPTV, if it use the default VLAN 1, this step could be ignored.



LAN Port Settings
The configuration takes effect only for the AP wit
Note: The configured LAN port settings prevail.

Default Settings

VLAN ID

(Range: 2-232 and 234-4090, WAN port.)

Applied to: AP device with no LAN port settings

LAN Port Settings

Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).

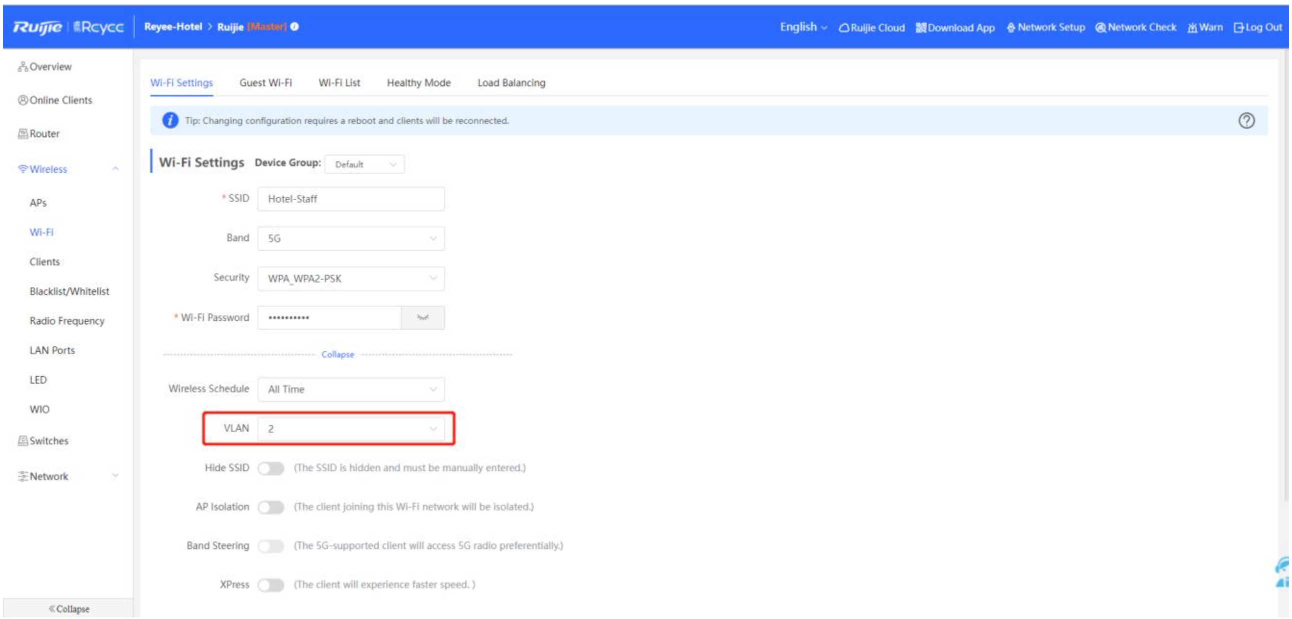
VLAN ID	Applied to	Action
No Data		

Add

VLAN ID: 100

* Applied to: G1QH26P01384A

Step5: Click **Wireless->Wi-Fi** to configure the WiFi for staff and guest. Choose VLAN 2 for Staff.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: Hotel-Staff

Band: 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••••

Collapse

Wireless Schedule: All Time

VLAN: 2

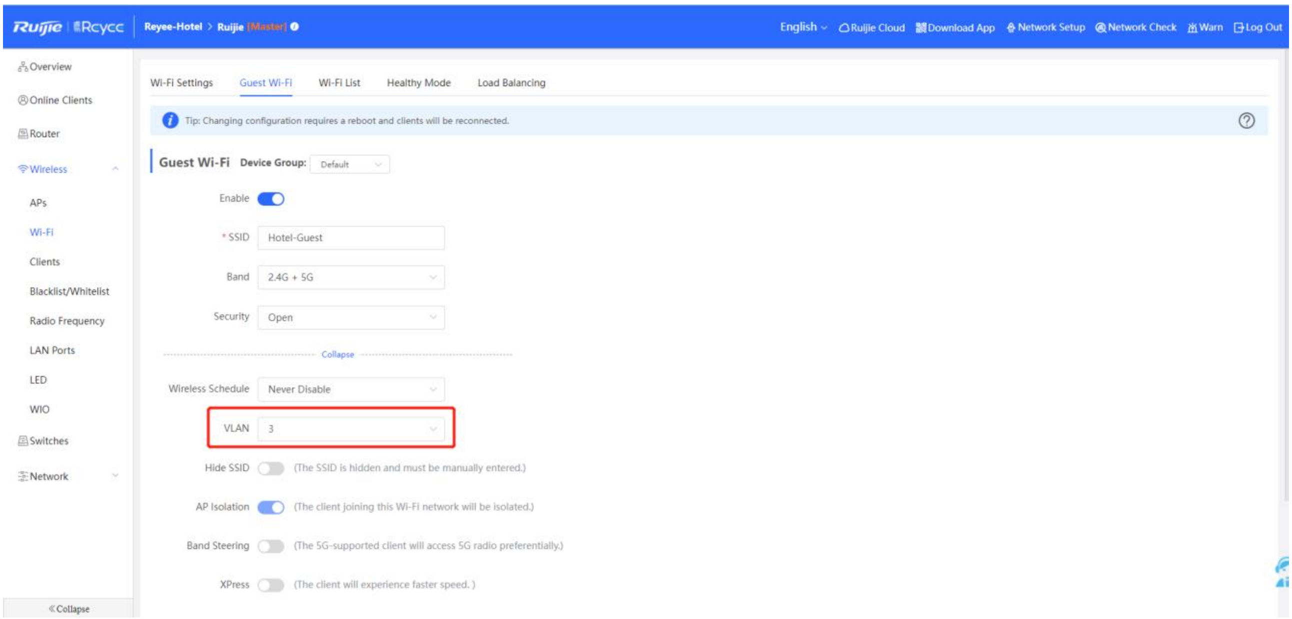
Hide SSID (The SSID is hidden and must be manually entered.)

AP Isolation (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)

XPress (The client will experience faster speed.)

Step6: Enable Guest WiFi, choose VLAN 3 for it.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable: on

* SSID: Hotel-Guest

Band: 2.4G + 5G

Security: Open

Collapse

Wireless Schedule: Never Disable

VLAN: 3

Hide SSID (The SSID is hidden and must be manually entered.)

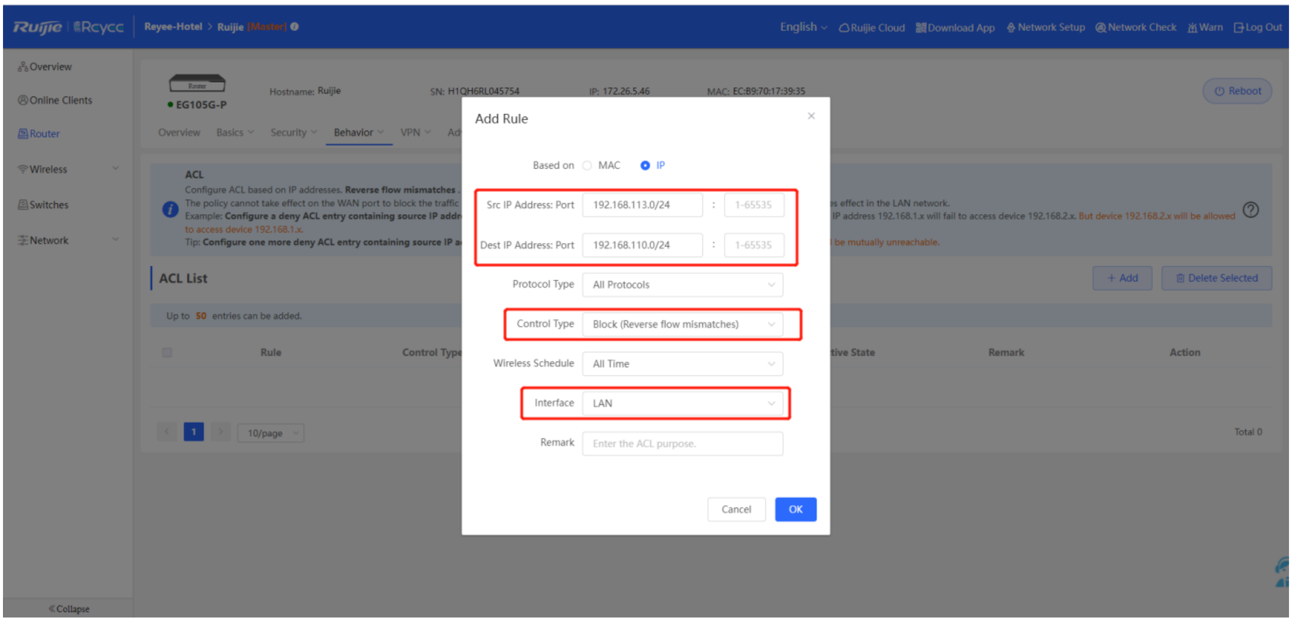
AP Isolation: on (The client joining this Wi-Fi network will be isolated.)

Band Steering (The 5G-supported client will access 5G radio preferentially.)

XPress (The client will experience faster speed.)

Step7: Click **Router->Behavior->Access Control, Configure ACL** to add ACL to block guest accessing to the internal network.

Add two ACLs to block VLAN 3 accessing to VLAN 1 & VLAN 2, this function is applied in LAN port.



Add Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.113.0/24 : 1-65535

Dest IP Address: Port 192.168.110.0/24 : 1-65535

Protocol Type All Protocols

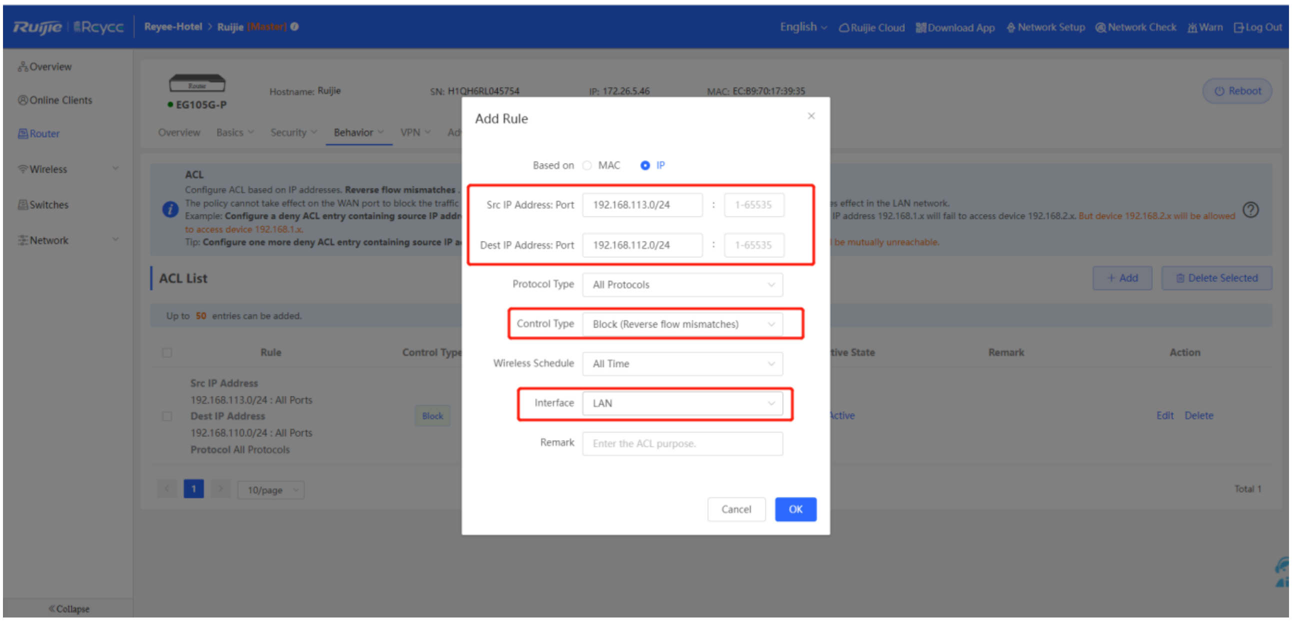
Control Type Block (Reverse flow mismatches)

Wireless Schedule All Time

Interface LAN

Remark Enter the ACL purpose.

Cancel OK



Add Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.113.0/24 : 1-65535

Dest IP Address: Port 192.168.112.0/24 : 1-65535

Protocol Type All Protocols

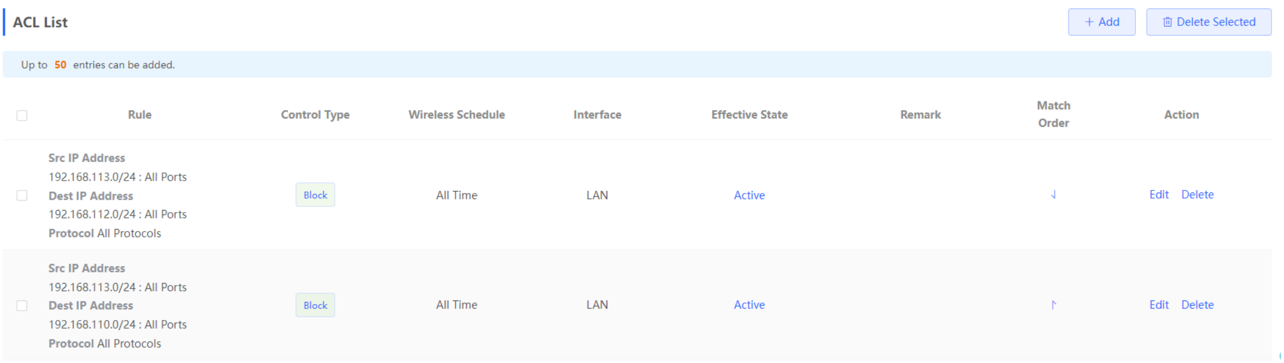
Control Type Block (Reverse flow mismatches)

Wireless Schedule All Time

Interface LAN

Remark Enter the ACL purpose.

Cancel OK



ACL List

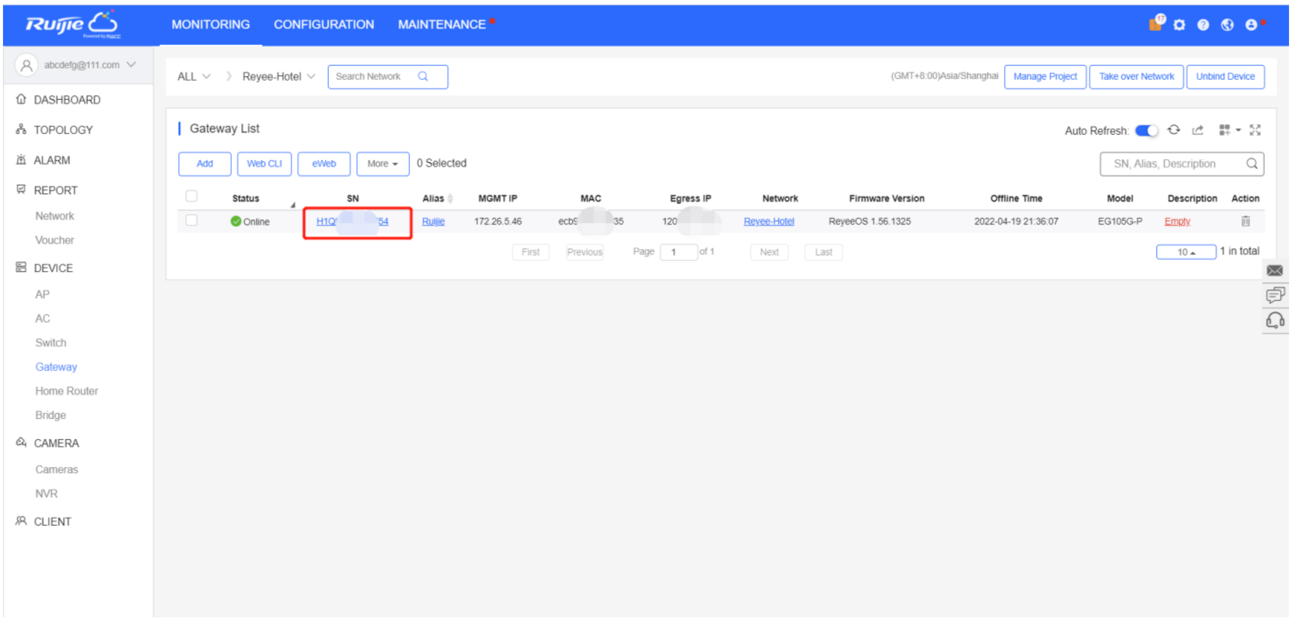
+ Add 🗑 Delete Selected

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	**Src IP Address** 192.168.113.0/24 : All Ports **Dest IP Address** 192.168.112.0/24 : All Ports **Protocol** All Protocols	Block	All Time	LAN	Active		↓	Edit Delete
□	**Src IP Address** 192.168.113.0/24 : All Ports **Dest IP Address** 192.168.110.0/24 : All Ports **Protocol** All Protocols	Block	All Time	LAN	Active		↑	Edit Delete

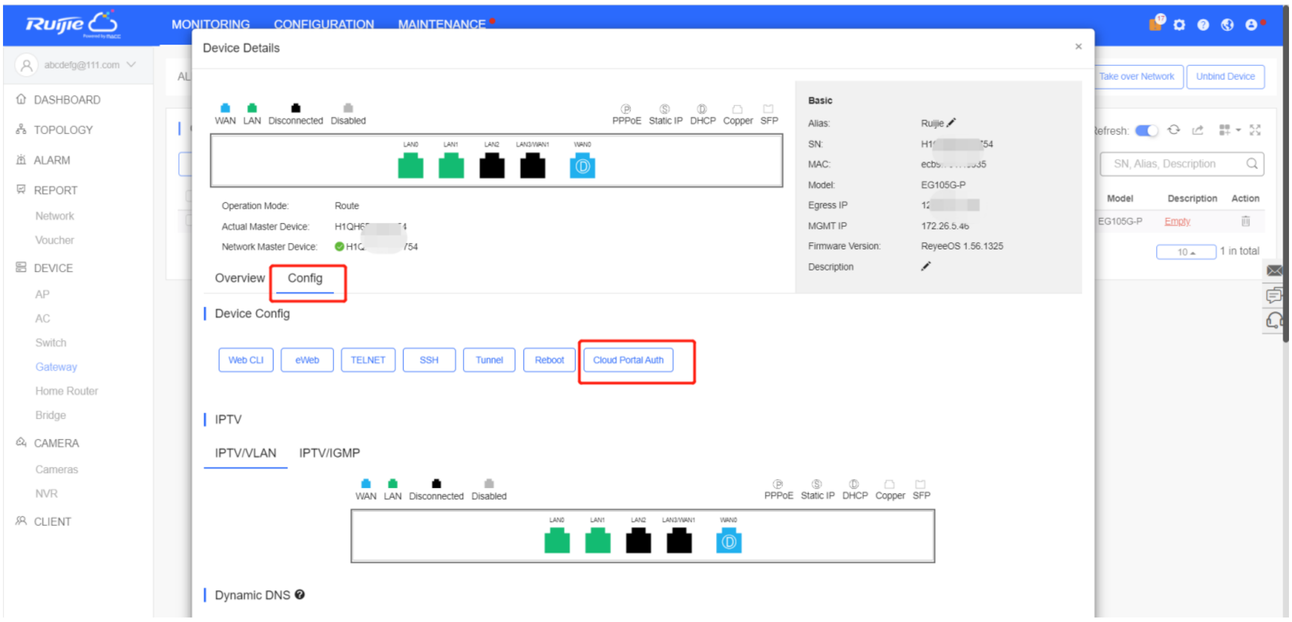
Step 8: Login to Cloud web to configure Cloud voucher authentication for guest.

Click the SN of the EG to enter its device detail page.



Status	SN	Alias	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Action
Online	H1Q[redacted]54	Ruijie	172.26.5.46	ecb[redacted]35	120[redacted]	Reyee-Hotel	ReyeeOS 1.56.1325	2022-04-19 21:36:07	EG105G-P	Empty	

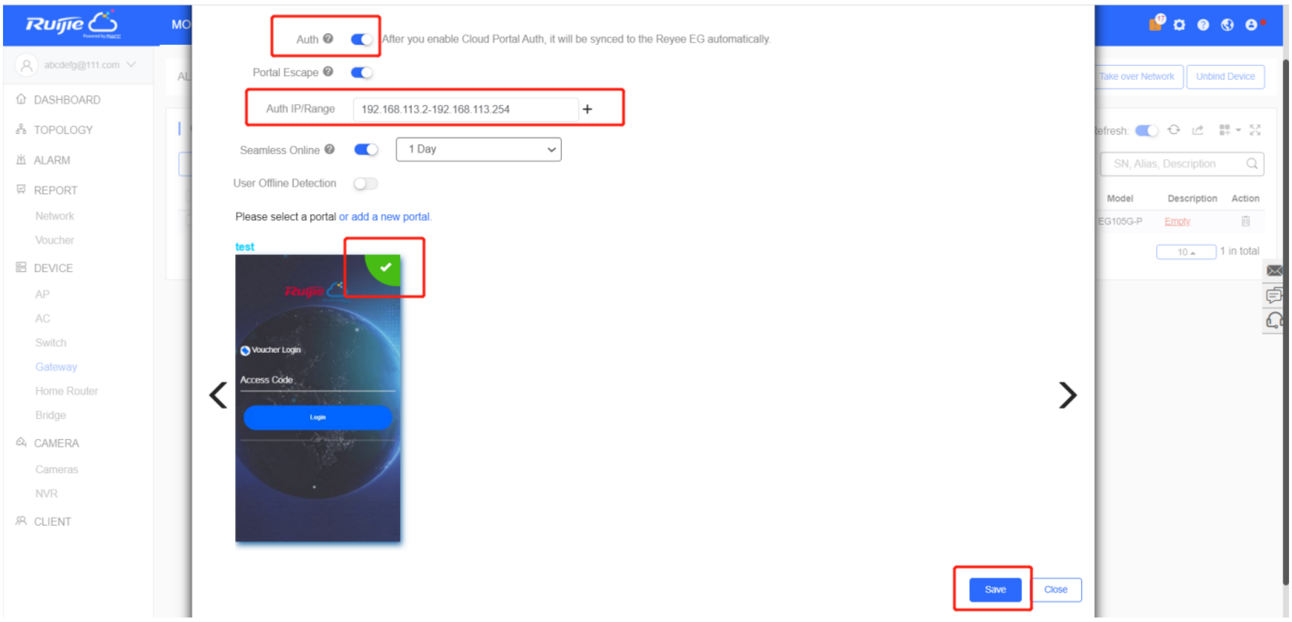
Click Config->Cloud Portal Auth



Operation Mode: Route
Actual Master Device: H1QH[redacted]4
Network Master Device: H1Q[redacted]754

Basic
Alias: Ruijie
SN: H1[redacted]54
MAC: ecb[redacted]35
Model: EG105G-P
Egress IP: 12[redacted]
MGMT IP: 172.26.5.46
Firmware Version: ReyeeOS 1.56.1325
Description:

Enable auth and configure the Guest clients IP range from 192.168.113.2 to 192.168.113.254.



Auth ✓ After you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.

Portal Escape ✓

Auth IP/Range: 192.168.113.2-192.168.113.254

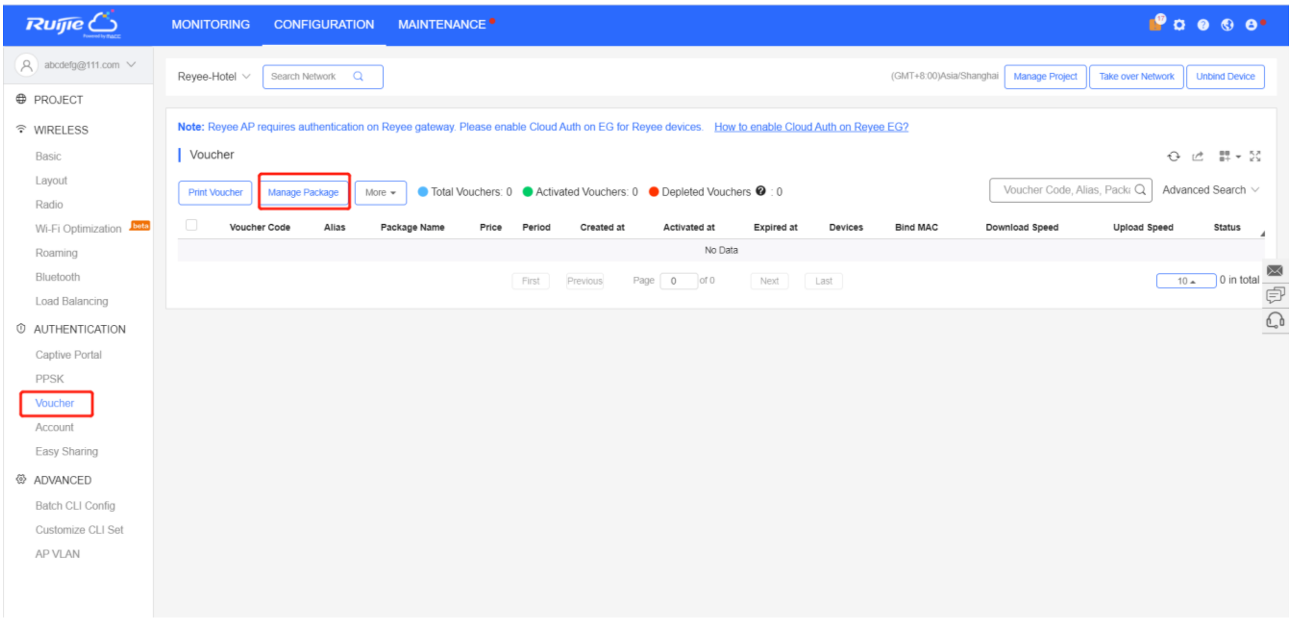
Seamless Online ✓ 1 Day

User Offline Detection ○

Please select a portal or add a new portal.

Add the voucher package for Guest

Click **Voucher->Manage Package->Add Package** to add voucher package for Guest.



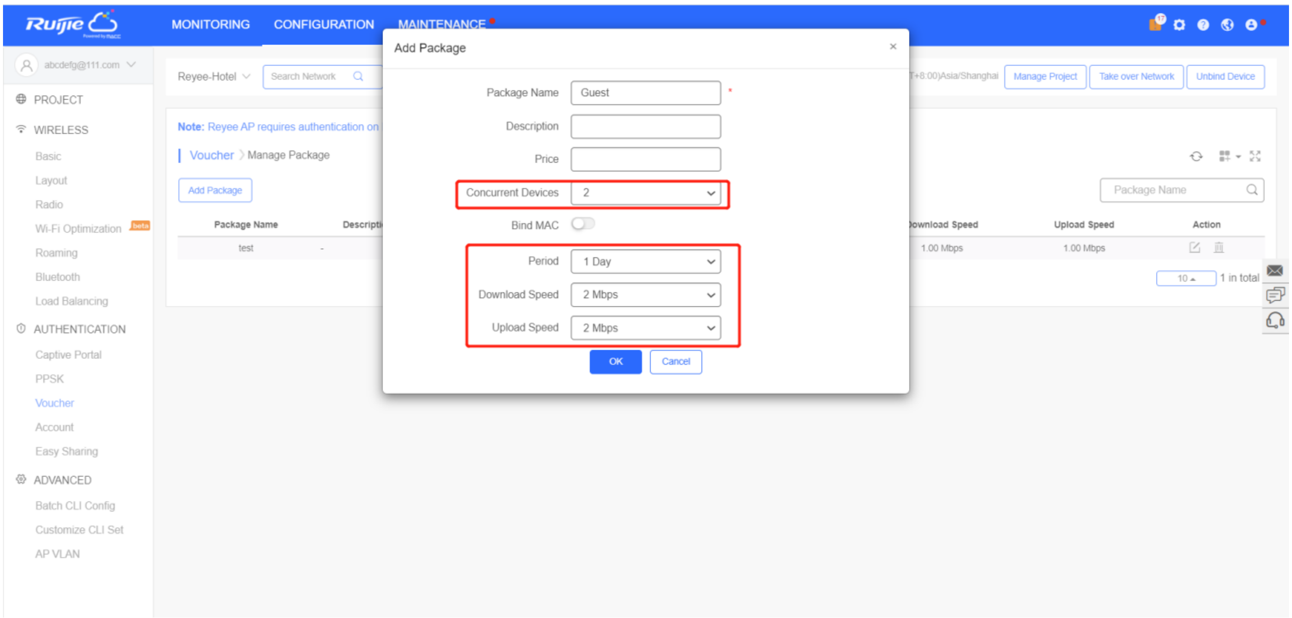
Note: Reyee AP requires authentication on Reyee gateway. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?

Voucher

Total Vouchers: 0 Activated Vouchers: 0 Depleted Vouchers : 0

□	Voucher Code	Alias	Package Name	Price	Period	Created at	Activated at	Expired at	Devices	Bind MAC	Download Speed	Upload Speed	Status
No Data													

Example: the **Concurrent Devices** to be 2, **Period** to be 1 day and the upload and download speed limitation to be 2Mbps.



Note: Reyee AP requires authentication on

Voucher > Manage Package

Package Name	Descripti...	...ownload Speed	Upload Speed	Action
test	-	1.00 Mbps	1.00 Mbps	

10 ▴ 1 in total

Add Package ×

Package Name: Guest *

Description:

Price:

Concurrent Devices: 2

Bind MAC: ○

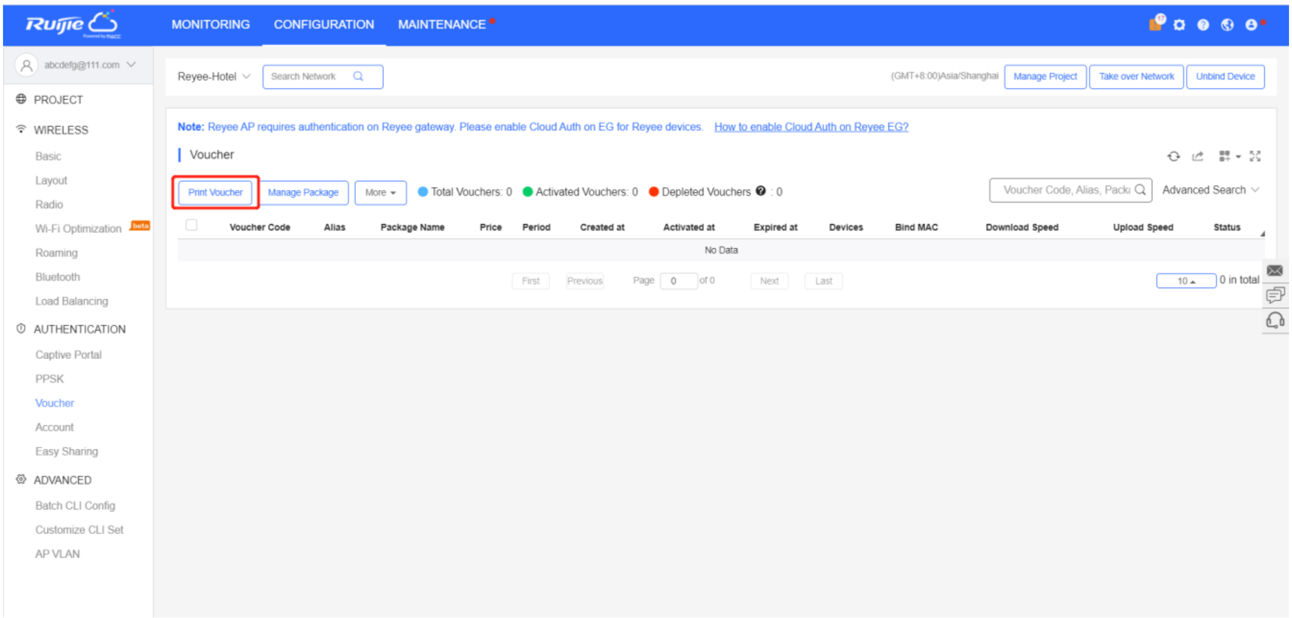
Period: 1 Day

Download Speed: 2 Mbps

Upload Speed: 2 Mbps

OK Cancel

Click **Print Voucher** to get one code for Guest.



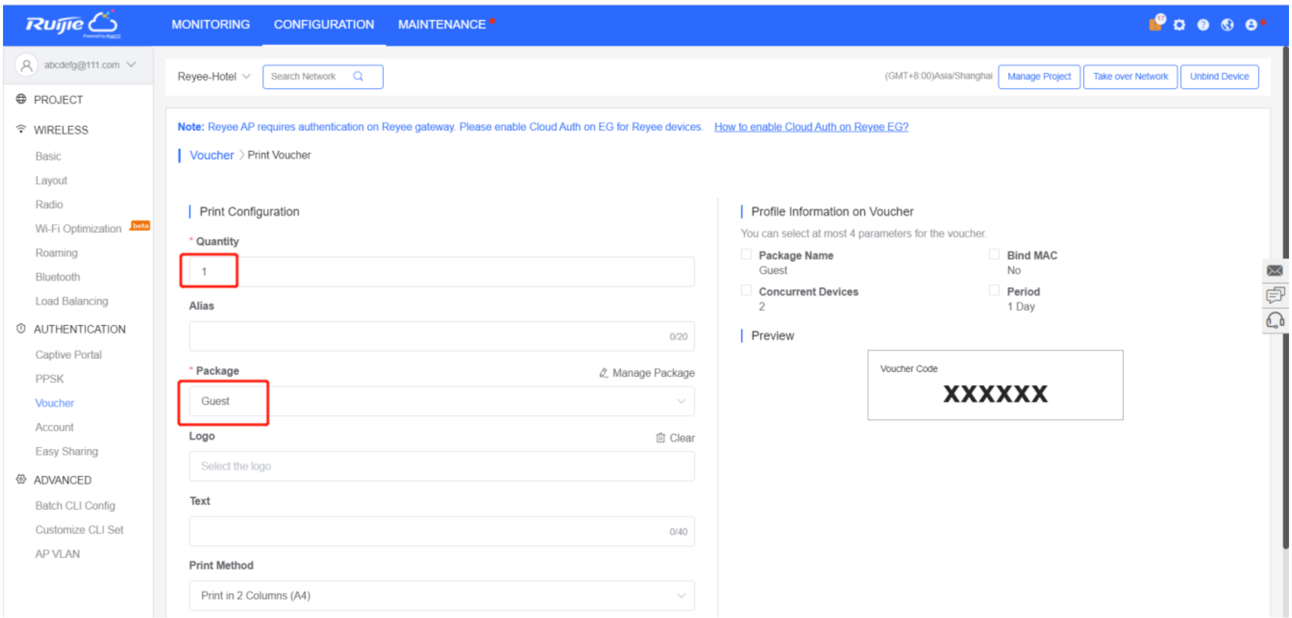
Note: Reyee AP requires authentication on Reyee gateway. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?

Voucher

● Total Vouchers: 0 ● Activated Vouchers: 0 ● Depleted Vouchers : 0

□	Voucher Code	Alias	Package Name	Price	Period	Created at	Activated at	Expired at	Devices	Bind MAC	Download Speed	Upload Speed	Status
No Data													

First Previous Page 0 of 0 Next Last 10 ▴ 0 in total



Note: Reyee AP requires authentication on Reyee gateway. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?

Voucher > Print Voucher

Print Configuration

* Quantity: 1

Alias: 0/20

* Package: Guest (Manage Package)

Logo: Select the logo (Clear)

Text: 0/40

Print Method: Print in 2 Columns (A4)

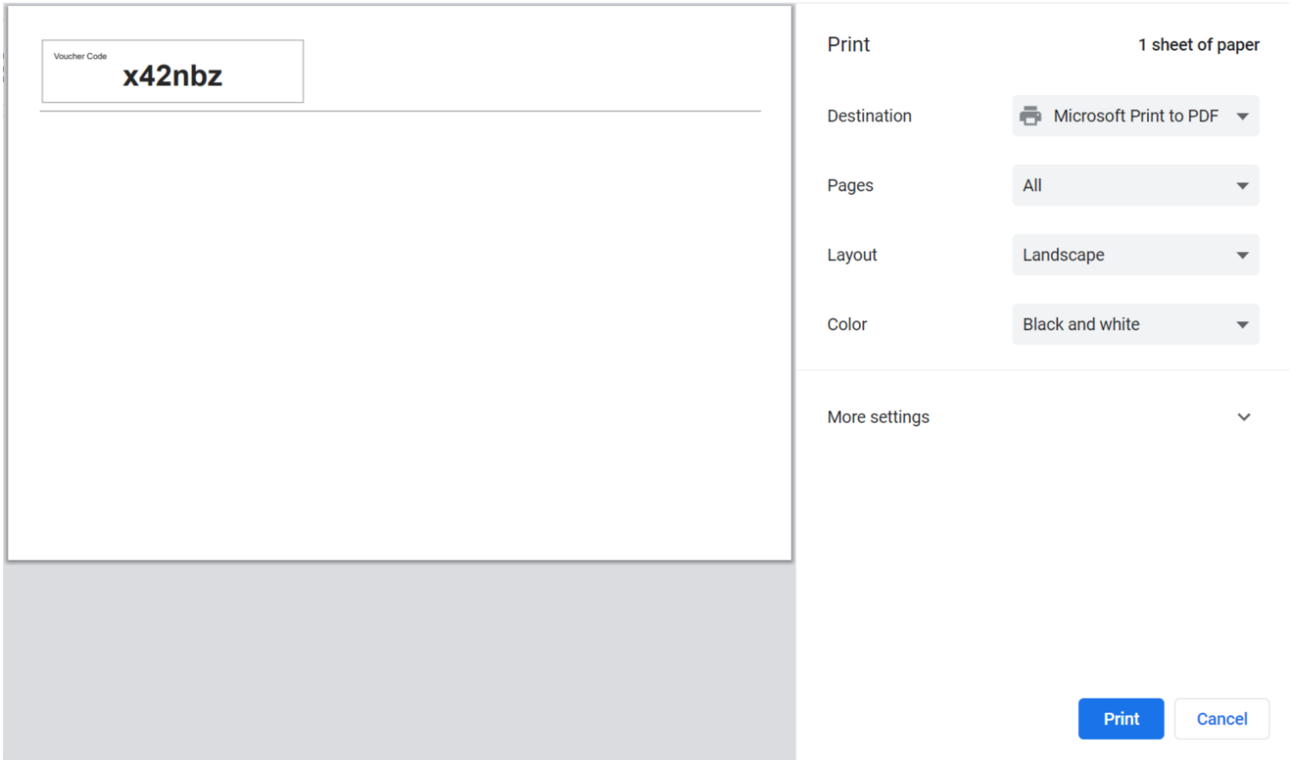
Profile Information on Voucher

You can select at most 4 parameters for the voucher.

□ Package Name Guest	□ Bind MAC No
□ Concurrent Devices 2	□ Period 1 Day

Preview

Voucher Code
XXXXXX



Voucher Code
x42nbz

Print 1 sheet of paper

Destination: Microsoft Print to PDF

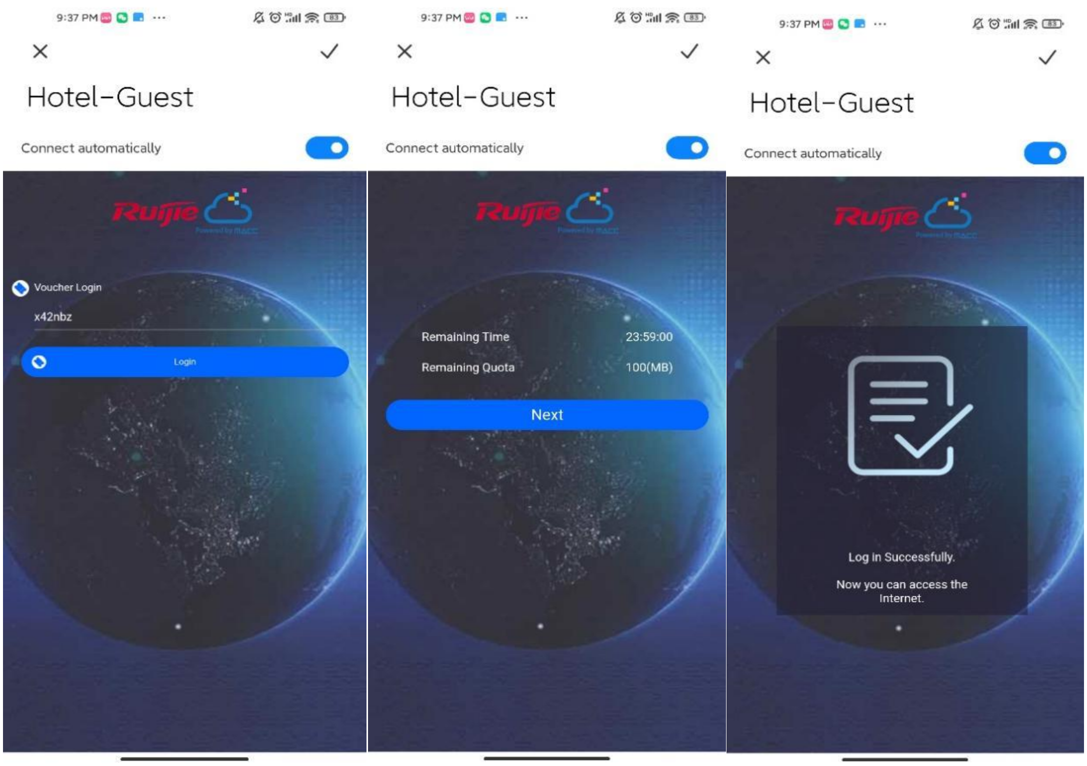
Pages: All

Layout: Landscape

Color: Black and white

Configuration Verification

Connect Guest WiFi, then you can see the internal IP 192.168.110.1 can not be accessed.



Hotel-Guest

Connect automatically

Voucher Login

x42nbz

Login

Hotel-Guest

Connect automatically

Remaining Time 23:59:00

Remaining Quota 100(MB)

Next

Hotel-Guest

Connect automatically

Log in Successfully.

Now you can access the Internet.

21 Reyee FAQ

21.1 Reyee Password FAQ ((collection))

21.2 Reyee Flow Control FAQ((collection))

21.3 Reyee Self-Organizing Network (SON) FAQ ((collection))

21.4 Reyee series Devices Parameters Tables

21.5 Reyee Parameter Consultation FAQ ((collection))