Ruijie RG-NBS3300 Series Switches

OS 2.273 Configuration Guide

Document Version: V1.0
Date: August 28, 2024

Copyright

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained 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

- Ruijie Networks website: https://www.ruijienetworks.com/
- Online support center: https://ruijienetworks.com/support
- Case portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Email support: service_rj@ruijienetworks.com
- Live chat: https://www.ruijienetworks.com/rita
- Documentation feedback: doc@ruijie.com.cn

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

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

✓ **Specification**

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

3. Note

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

Contents

1 Change Description

This chapter describes the major changes in software and hardware of different versions and related documentation. For details about hardware changes, see the release notes published with software versions.

1.1 OS 2.273

1.1.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
RG-NBS3300-8MG2XS-P	V1.0x
RG-NBS3300-16MG4XS-HP	V1.0x

1.1.2 Software Feature Change

This baseline version has no software feature change.

2 Login

2.1 Configuration Environment Requirements

- Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble characters or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Logging in to the Web Interface

2.2.1 Connecting to the Device

Use an Ethernet cable to connect the switch port to the Ethernet port of the PC, and configure an IP address for the PC that is on the same network segment as the default IP of the device to ensure that the PC can ping the switch. For example, set the IP address of the PC to 10.44.77.100.

Table 2-1 Default Settings

Feature	Default Value
Device IP Address	10.44.77.200
Password	A username is not required when you log in for the first time. The default password is "admin".

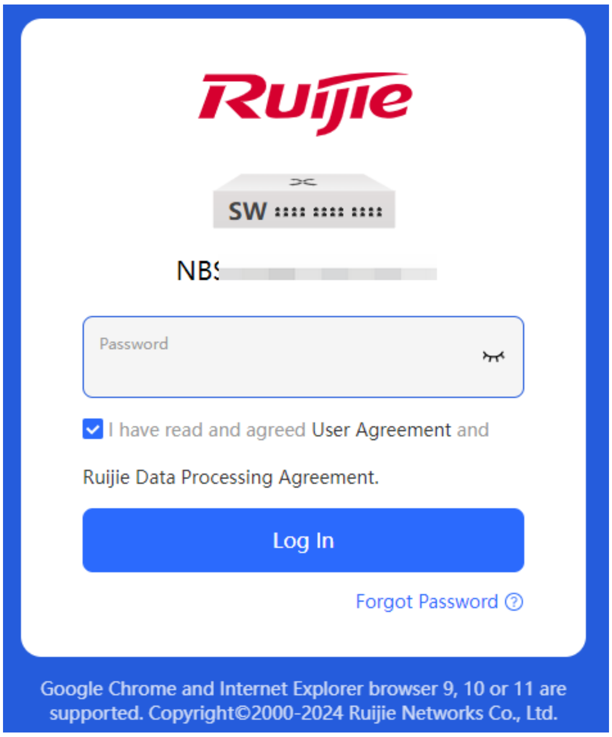
2.2.2 Logging in to the Web Interface

(1) Enter the IP address (10.44.77.200 by default) of the device in the address bar of the browser to access the login page.

Note

If the static IP address of the device is changed, or the device dynamically obtains a new IP address, the new IP address can be used to access the web management system of the device as long as the PC and the device are on the same LAN, and their IP addresses are in the same network segment.

(2) Enter the password and click **Log In** to access the homepage of the web management system.



☑ I have read and agreed User Agreement and Ruijie Data Processing Agreement.

Google Chrome and Internet Explorer browser 9, 10 or 11 are supported. Copyright©2000-2024 Ruijie Networks Co., Ltd.

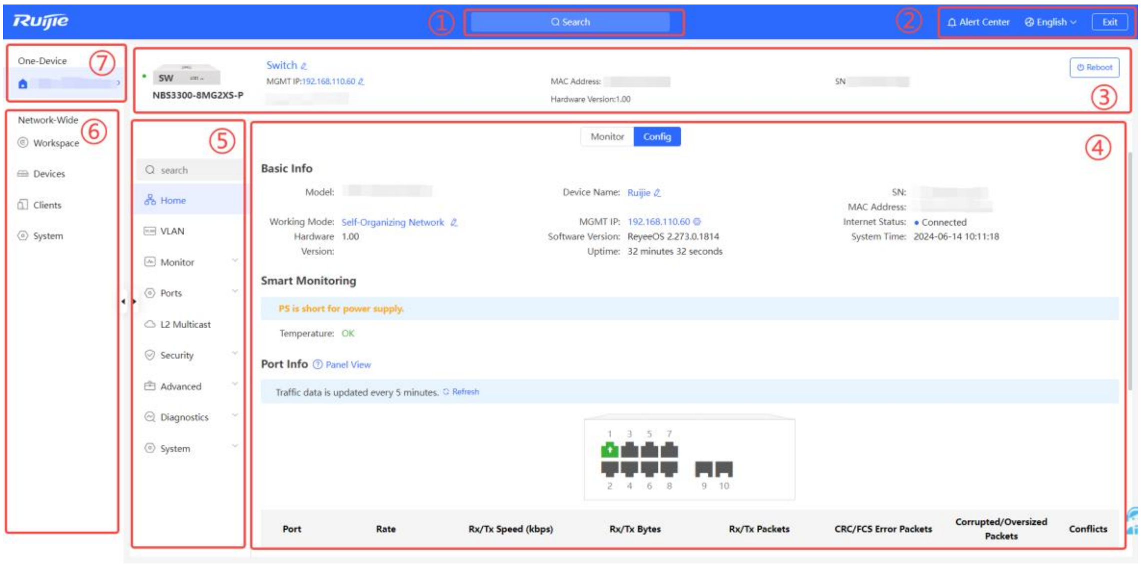
You can use the default password admin to log in to the device for the first time. For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

If you forget the device IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to a power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

Caution

- Restoring factory settings will delete all configurations of the device. Therefore, exercise caution when performing this operation.
- The method to restore factory settings may vary with devices. For details, see the installation guide for specific instructions.

2.2.3 Layout Configuration



MGMT IP:192.168.110.60

MAC Address:

Hardware Version:1.00

SN

Basic Info

Model:

Working Mode: Self-Organizing Network

Hardware Version: 1.00

Device Name: Ruijie

MGMT IP: 192.168.110.60

Software Version: ReyeeOS 2.273.0.1814

Uptime: 32 minutes 32 seconds

SN:

MAC Address:

Internet Status: ● Connected

System Time: 2024-06-14 10:11:18

Smart Monitoring

PS is short for power supply.

Temperature: OK

Port Info

Traffic data is updated every 5 minutes.

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts

Table 2-2 Layout Configuration

No.	Description
1	Search for frequently used device functions, including network-wide management, egress gateway, and device and system related functionalities.
2	Quick view of device alarms, change the web interface language, and exit the web interface.
3	Device information and device restart button.
4	Device function configuration and display area. Click **Monitor** to display the interface traffic and PoE power usage of the device (only PoE switches with model names containing –P, -LP, -HP, and -UP support this function). Click **Config** to view the device's configuration and running status.
5	The navigation bar, which is vertically arranged on the left side when the device is a primary device on the network, and is horizontally arranged on the top when the device is a secondary device.
6	Frequently used functions of all wired and wireless Ruijie products on self-organizing network, which can be configured in batch.
7	In this pane, you can configure all functions of the local device, as well as rapid setup of the egress gateway.

2.3 Quick Setup

2.3.1 Configuration Preparations

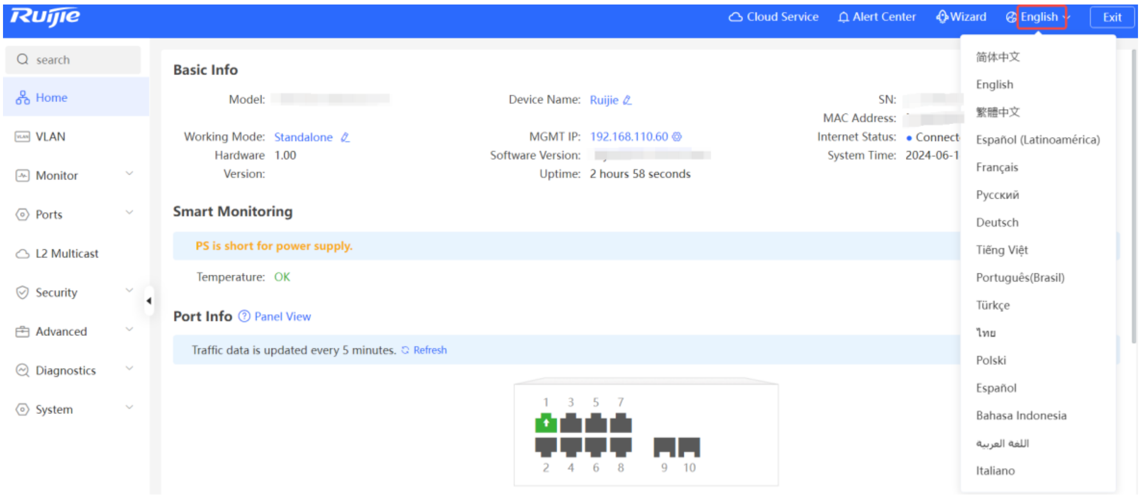
Connect the device to the power supply, and connect the device port to an uplink device with an Ethernet cable.

2.3.2 Procedure

1. Change the Web Interface Language

Click **English** in the top right corner of the web interface.

Select the desired language from the drop-down list to change the language of the web interface.



Basic Info

Model: [redacted]
Device Name: Ruijie
SN: [redacted]
MAC Address: [redacted]
Working Mode: Standalone
MGMT IP: 192.168.110.60
Internet Status: ● Connect
Hardware Version: 1.00
Software Version: [redacted]
System Time: 2024-06-1
Uptime: 2 hours 58 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK

Port Info Panel View

Traffic data is updated every 5 minutes. Refresh

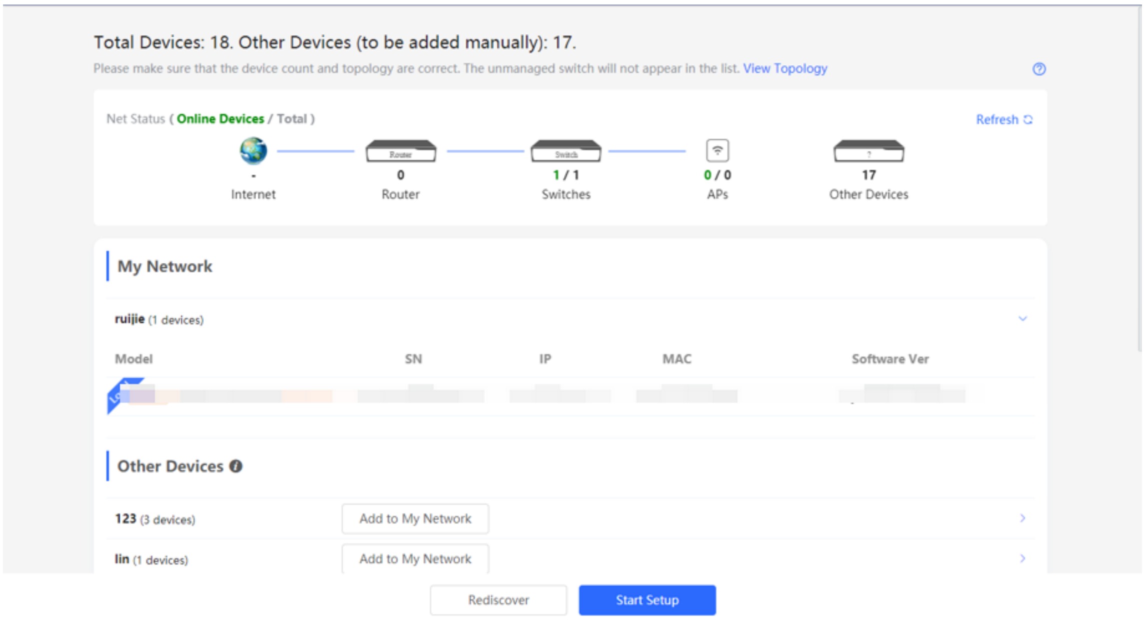
2. Adding a Device to the Network

By default, users can perform batch settings and centralized management of all devices on the network. Therefore, before starting configuration, you need to check and confirm the number of online devices and their connection status on the network.

Note

Under normal circumstances, when multiple new devices are powered on and connected, they will be automatically interconnected into a network, and the user only needs to confirm that the number of devices is correct.

If there are other devices on the network that are not added to the current network, you can manually add them by choosing **Workspace** > **Quick Setup** > **Add to My Network** on the network-wide section and entering the management password of each device. This will incorporate the respective devices into the appropriate network, allowing you to proceed with the network-wide configuration.



Total Devices: 18. 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

My Network

ruijie (1 devices)

Model	SN	IP	MAC	Software Ver

Other Devices

123 (3 devices) Add to My Network

lin (1 devices) Add to My Network

3. Creating a Web Project

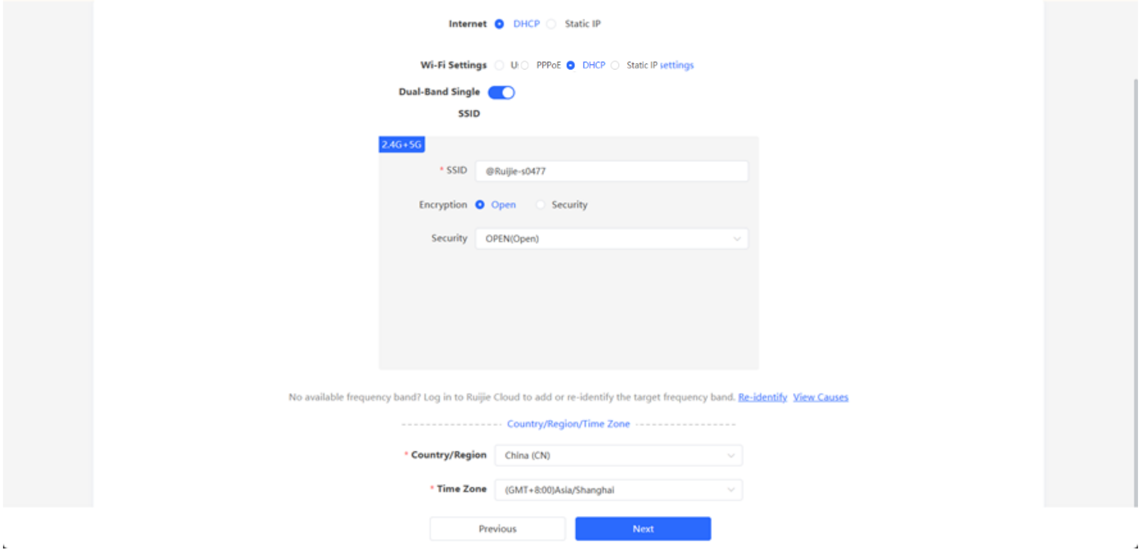
(1) Click **Start Setup** to configure the Internet connection type.

- **Internet**: Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
  - PPPoE: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.

  DHCP: The device detects whether it can obtain an IP address via DHCP by default. If the device connects to the Internet successfully, you can click **Next** without entering an account.

  Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

- **Wi-Fi Settings**: Select the Wi-Fi mode. This configuration option is unavailable for a new project.
  - Use old settings: Use the Wi-Fi settings of an existing project.
  - Use new settings: Configure the Wi-Fi network using new settings.
- **SSID and Wi-Fi Password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.
- **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Time Zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.



Internet ● DHCP ○ Static IP

Wi-Fi Settings ○ U ○ PPPoE ● DHCP ○ Static IP settings

Dual-Band Single SSID

2.4G+5G

* SSID: @Ruijie-s0477

Encryption ● Open ○ Security

Security: OPEN(Open)

No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. Re-identify View Causes

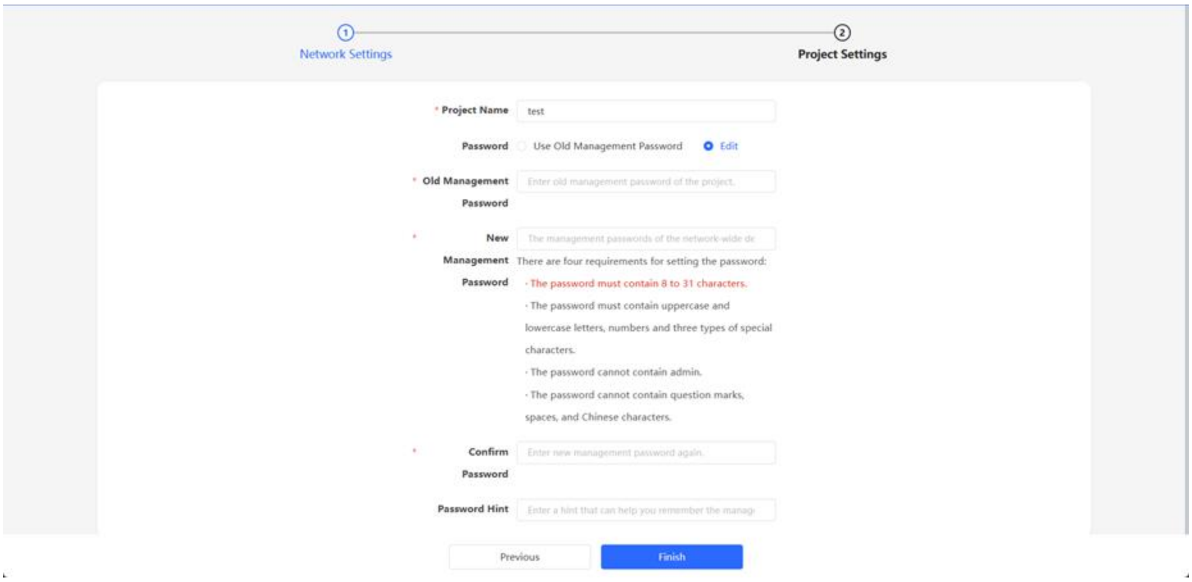
Country/Region/Time Zone

* Country/Region: China (CN)

* Time Zone: (GMT+8:00)Asia/Shanghai

(2) Click **Next**. On the page that is displayed, set the project name and management password.

- **Project Name**: Identifies the network project where the device is located.
- **Management Password**: The password is used for logging in to the web interface.



* Project Name: test

Password ○ Use Old Management Password ● Edit

* Old Management Password: Enter old management password of the project.

* New Management Password: The management passwords of the network-wide de

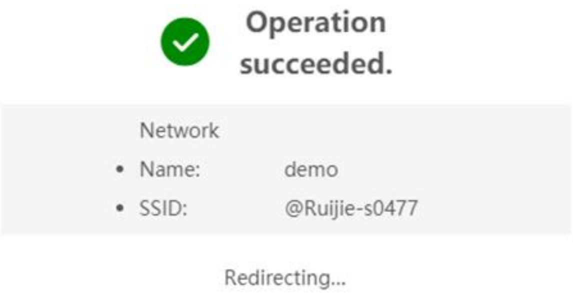
There are four requirements for setting the password:

- The password must contain 8 to 31 characters.
- The password must contain uppercase and lowercase letters, numbers and three types of special characters.
- The password cannot contain admin.
- The password cannot contain question marks, spaces, and Chinese characters.

* Confirm Password: Enter new management password again.

Password Hint: Enter a hint that can help you remember the manag

Click **Finish**. The system will deliver the initialization settings to the device and check the network connectivity.



Operation succeeded.

Network

- Name: demo
- SSID: @Ruijie-s0477

Redirecting...

The device can access the Internet now. Bind the device to a Ruijie Cloud account for remote management. Follow the instruction to log in to Ruijie Cloud for further configuration.

Note

- If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.
- Log in again with the new password if you change the management password.

2.4 Work Mode

The device supports two work modes: **Standalone** and **Self-Organizing Network**. It works in **Self-Organizing Network** mode by default. The system presents different menu items based on the work mode. To modify the work mode, see Switching the Work Mode.

Self-Organizing Network: After the self-organizing network discovery function is enabled, the device can be discovered on the network and discover other devices on the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of the device to check management information about all devices on the network. After self-organizing network discovery is enabled, users can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

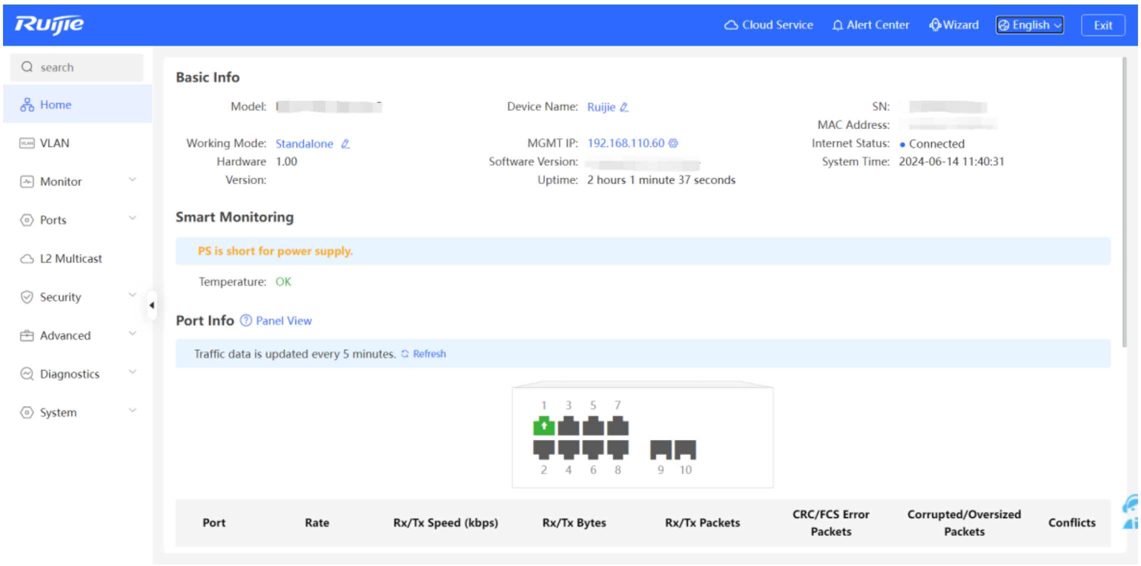
When the device is in self-organizing network mode, the web interface has two configuration modes: the network wide management mode and the local device mode. For more information, see 2.5 Switching the Management Mode.

Standalone mode: If the self-organizing network discovery function is disabled, the device will not be discovered on the network. After logging in to the web interface, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

2.5 Switching the Management Mode

In standalone mode, you can configure and manage only the current logged in device without self-organizing network function, as shown in Figure 2-1.

Figure 2-1 Web Interface in Standalone Mode



Basic Info

Model: [redacted]
Device Name: Ruijie
SN: [redacted]
MAC Address: [redacted]
Working Mode: Standalone
MGMT IP: 192.168.110.60
Internet Status: ● Connected
Hardware Version: 1.00
Software Version: [redacted]
System Time: 2024-06-14 11:40:31
Uptime: 2 hours 1 minute 37 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK

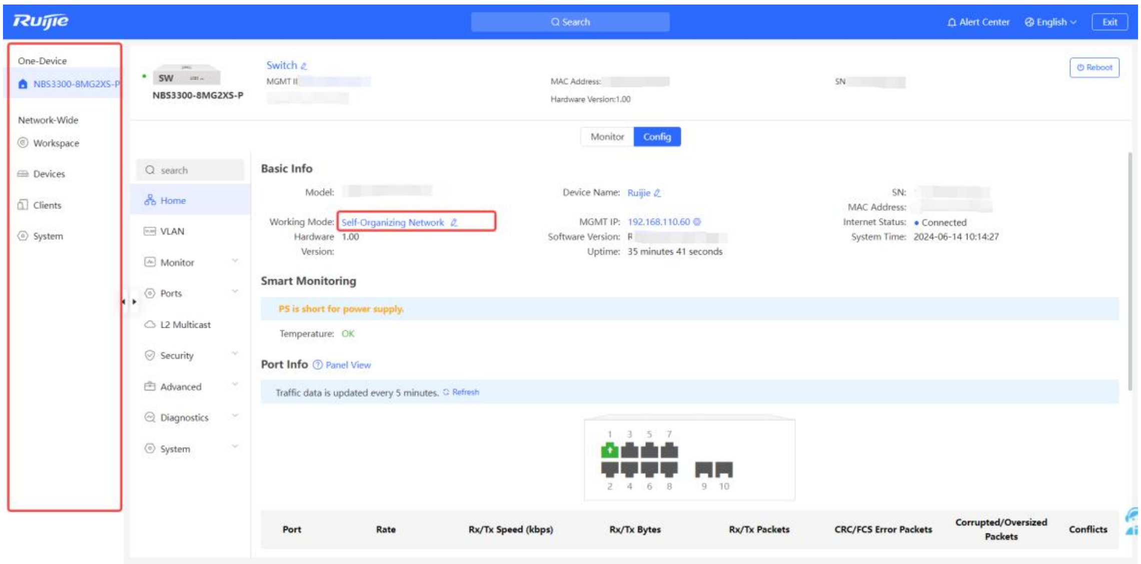
Port Info Panel View

Traffic data is 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

In SON mode, you can batch set the commonly used functions of all wired and wireless Ruijie products on the self-organizing network, including the currently logged-in device, as shown in Figure 2-2.

Figure 2-2 Web Interface in Self-Organizing Mode



Switch
MGMT IP: [redacted]
MAC Address: [redacted]
Hardware Version:1.00
SN: [redacted]

Basic Info

Model: [redacted]
Device Name: Ruijie
SN: [redacted]
MAC Address: [redacted]
Working Mode: Self-Organizing Network
MGMT IP: 192.168.110.60
Internet Status: ● Connected
Hardware Version: 1.00
Software Version: [redacted]
System Time: 2024-06-14 10:14:27
Uptime: 35 minutes 41 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK

Port Info Panel View

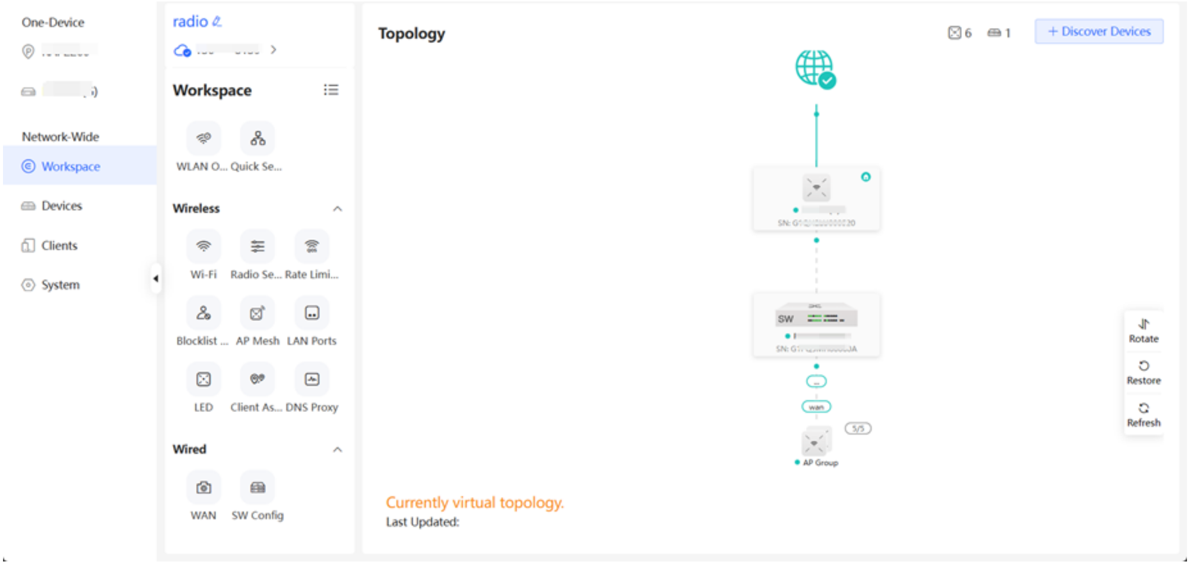
Traffic data is updated every 5 minutes. Refresh

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts

3 Network-Wide Management

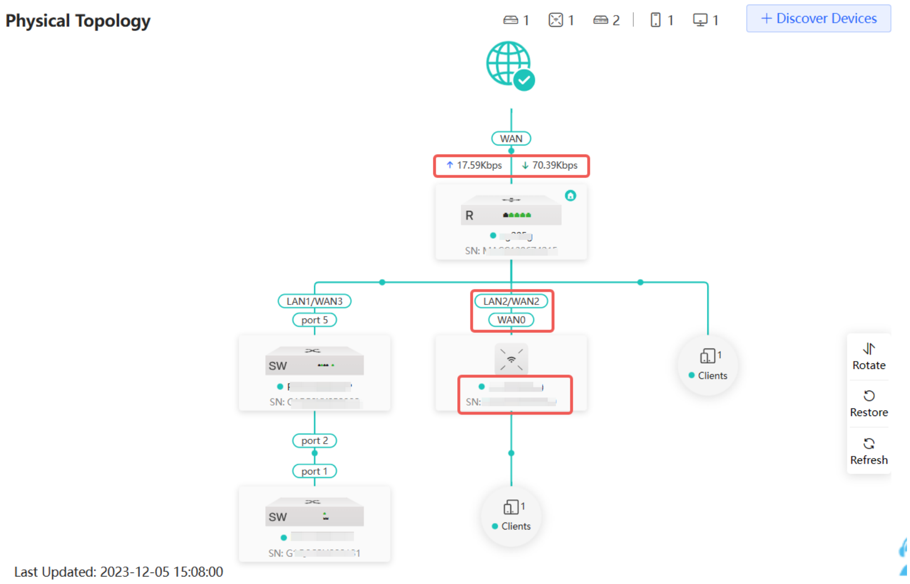
Choose **Network-Wide > Workspace** > **Topology**.

The **Topology** page displays the current network topology, real-time uplink and downlink traffic, connection status, and number of clients on the current network. It also provides quick actions for network and device setup. On the current page, you can monitor, configure, and manage the entire network.

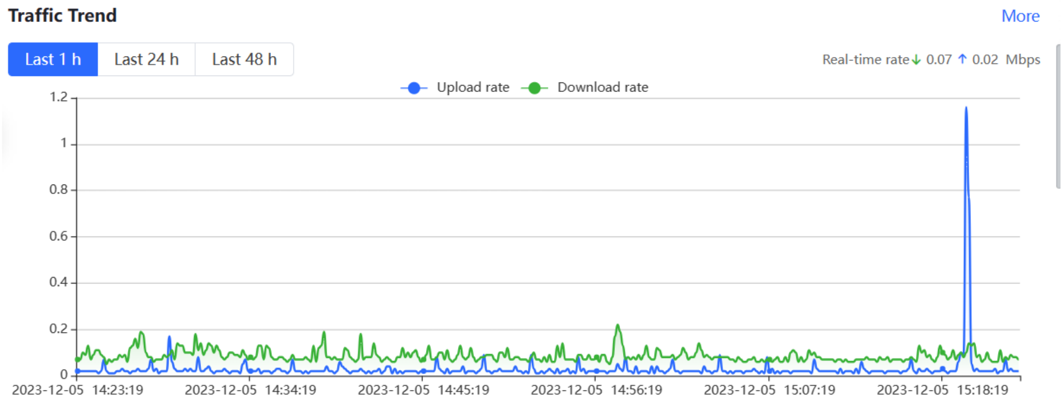


3.1 Viewing Networking Information

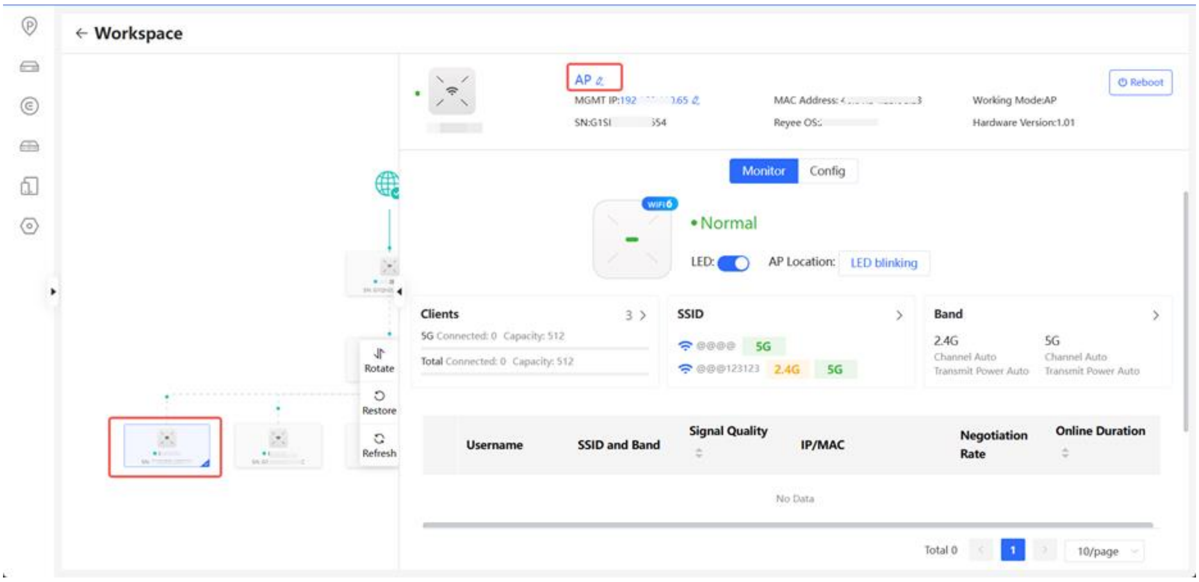
In SON mode, the topology displays information about online devices, connected ports, device SNs, and uplink and downlink real-time traffic.



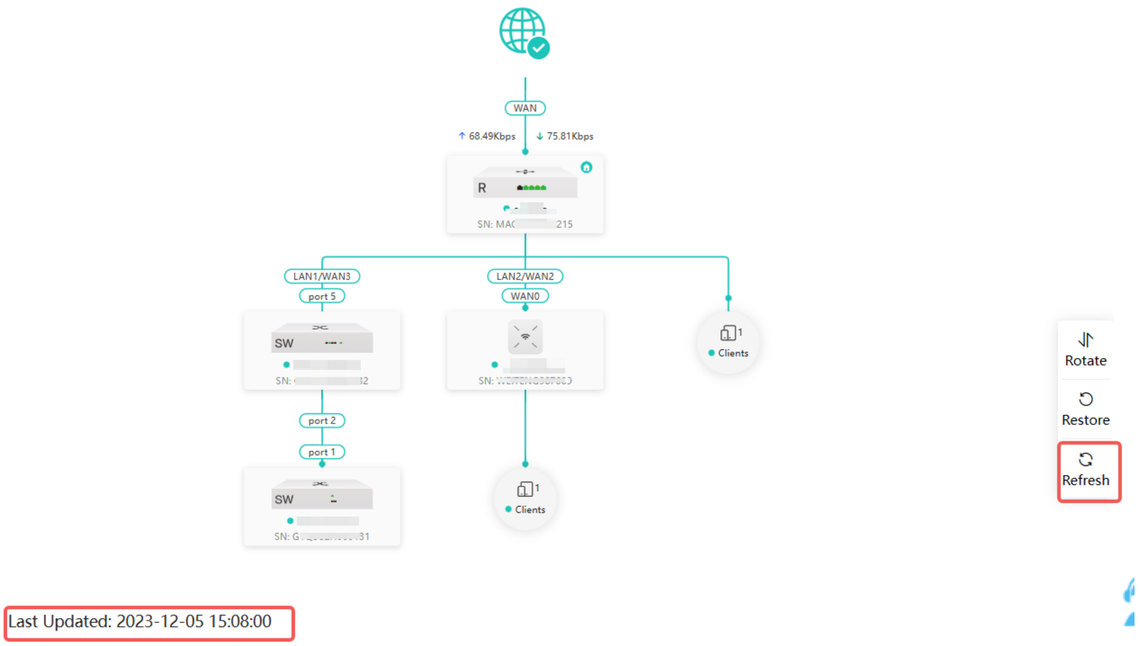
- Click the egress gateway to view real-time traffic information of the device.



- Click a device in the topology to view the running status and configuration of the device, and to configure functions on the device. The device name is the product model by default. You can click ✎ to change the device name.



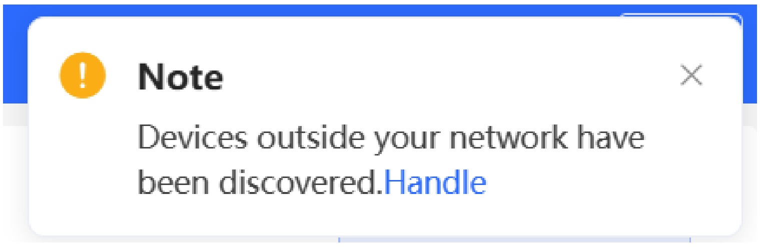
- The update time is displayed in the lower left corner of the topology page. Click **Refresh** to refresh the topology. It takes some time to refresh the topology.



3.2 Adding Devices

3.2.1 Adding a Device Through Wired Connection

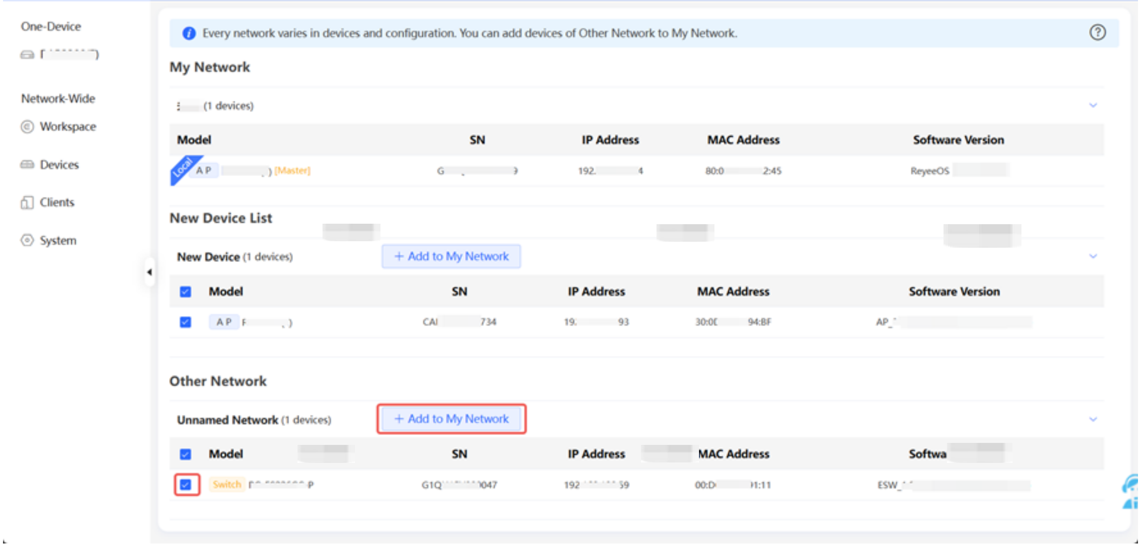
(1) When a new device joins the network through a wired connection, the system displays a prompt that a device not in SON is detected. Click **Handle** to add the device to the current network.



Note

Devices outside your network have been discovered.Handle

(2) On the **Network List** page, click the downward arrow next to **Other Network** to expand this list. Select the desired device(s) and click **Add to My Network**.



Every network varies in devices and configuration. You can add devices of Other Network to My Network.

My Network

(1 devices)

Model	SN	IP Address	MAC Address	Software Version
Local AP) [Master]	G	192. 4	80:0 2:45	ReyeeOS

New Device List

New Device (1 devices)

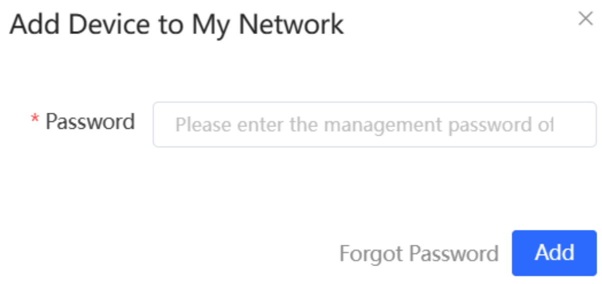
☑	Model	SN	IP Address	MAC Address	Software Version
☑	AP F)	CAI 734	19. 93	30:0[94:BF	AP_

Other Network

Unnamed Network (1 devices)

☑	Model	SN	IP Address	MAC Address	Softwa
☑	Switch P	G1Q 047	192 59	00:D 1:11	ESW_

You do not need to enter the password if the device to be added has not been configured before. If a password is required, enter the management password of the device. The device cannot be added if the entered management password is incorrect.



* Password: Please enter the management password of

3.2.2 AP Mesh

Note

This function is only supported on Ruijie APs that support AP Mesh function.

1. Overview

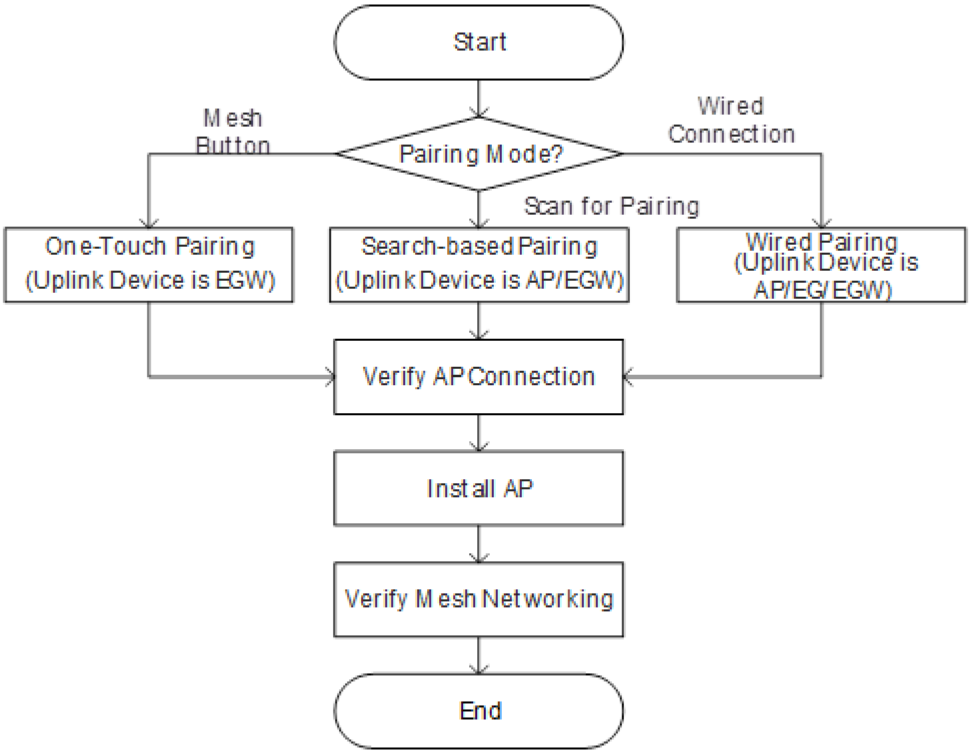
After being powered on and enabled with the AP Mesh feature, a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will synchronize its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

- One-touch pairing: Short press the Mesh button on the EGW router on the target network to implement fast pairing of the AP with the EGW router.
- Search-based pairing: Log in to the web interface of a device on the target network. Search and add APs to be paired.

- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

Once the pairing process is complete, the new AP acquires wireless backhaul information from neighboring APs within the network. After the new AP is installed, it will automatically connect to the most suitable neighboring AP.

2. Configuration Steps


Start
Pairing Mode?
Mesh Button
Wired Connection
Scan for Pairing
One-Touch Pairing (Uplink Device is EGW)
Search-based Pairing (Uplink Device is AP/EGW)
Wired Pairing (Uplink Device is AP/EG/ EGW)
Verify AP Connection
Install AP
Verify Mesh Networking
End

3. One-Touch Pairing

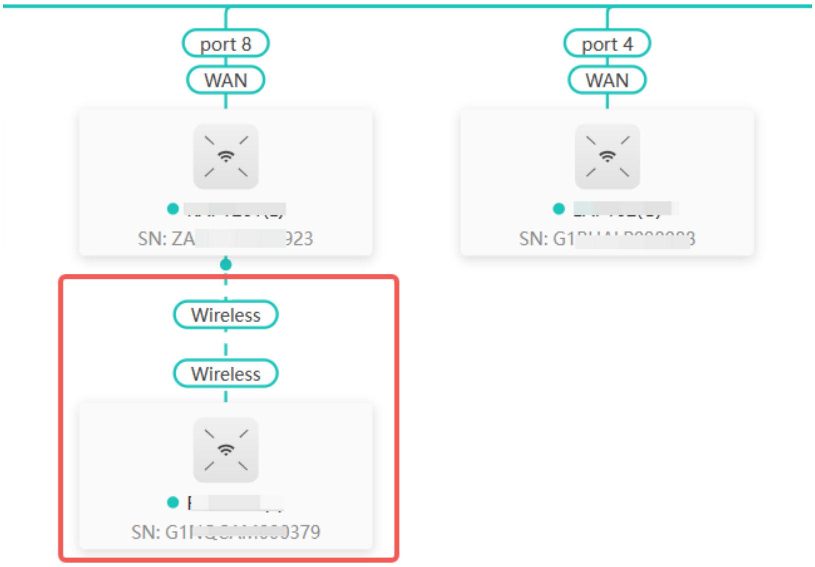
Caution

- The uplink device must be an EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the network is enabled with AP Mesh.
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the EGW router on the target network.

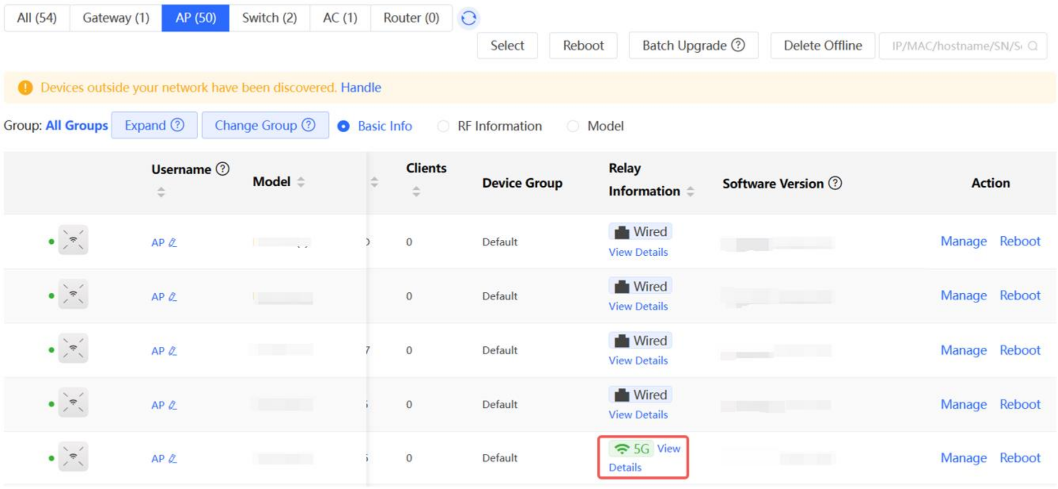
(2) Press and hold the Mesh button on the EGW router for no more than two seconds to start pairing. The pairing process takes about one minute.

(3) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.



(4) Power off the new AP and install it to a planned location.

(5) Log in to the web interface of a device on the target network. In SON mode, choose **Devices** > **AP**. Make sure that the new AP is online and the icon 5G appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

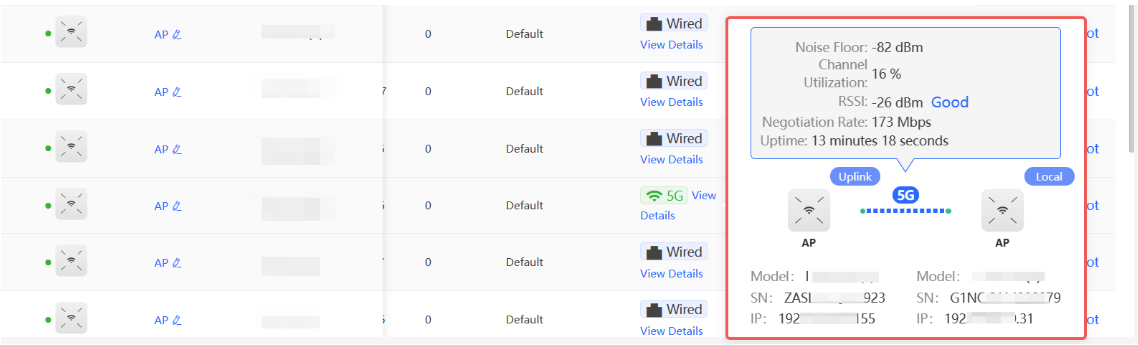


Devices outside your network have been discovered. Handle

Group: All Groups Expand Change Group ● Basic Info ○ RF Information ○ Model

	Username	Model	Clients	Device Group	Relay Information	Software Version	Action
●	AP		0	Default	Wired View Details		Manage Reboot
●	AP		0	Default	Wired View Details		Manage Reboot
●	AP		0	Default	Wired View Details		Manage Reboot
●	AP		0	Default	Wired View Details		Manage Reboot
●	AP		0	Default	5G View Details		Manage Reboot

(6) Click **View Details** next to the 5G icon to obtain information about the uplink device and RSSI.



AP	0	Default	Wired View Details	ot
AP	0	Default	Wired View Details	ot
AP	0	Default	Wired View Details	ot
AP	0	Default	5G View Details	ot
AP	0	Default	Wired View Details	ot
AP	0	Default	Wired View Details	ot

Noise Floor: -82 dBm
Channel Utilization: 16 %
RSSI: -26 dBm Good
Negotiation Rate: 173 Mbps
Uptime: 13 minutes 18 seconds

Model: I
SN: ZASI 923
IP: 192 155

Model:
SN: G1NC 79
IP: 192 .31

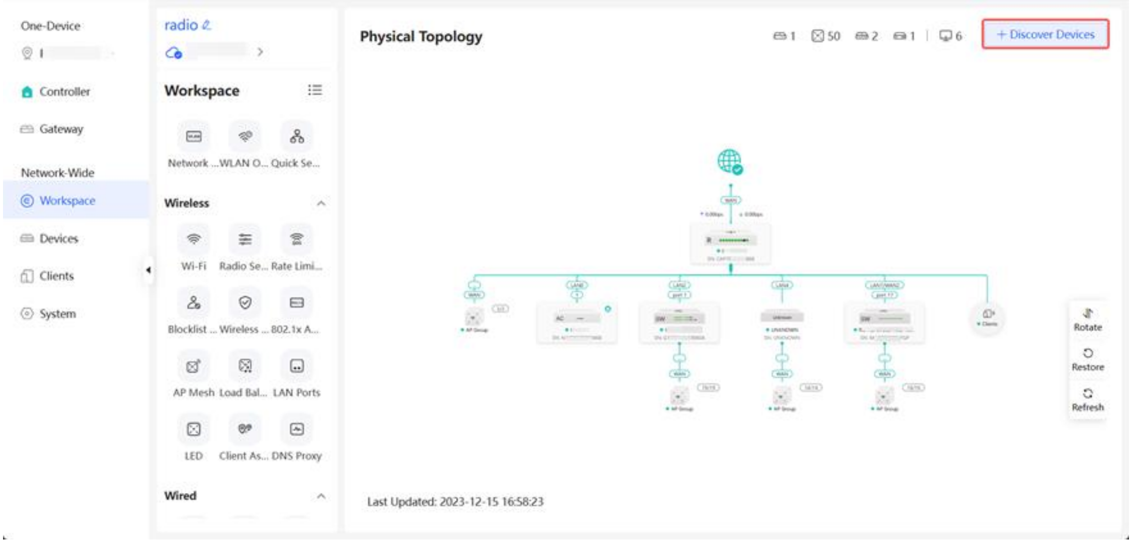
4. Search-based Pairing

Caution

- The uplink device must be an EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the network is enabled with AP Mesh.
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

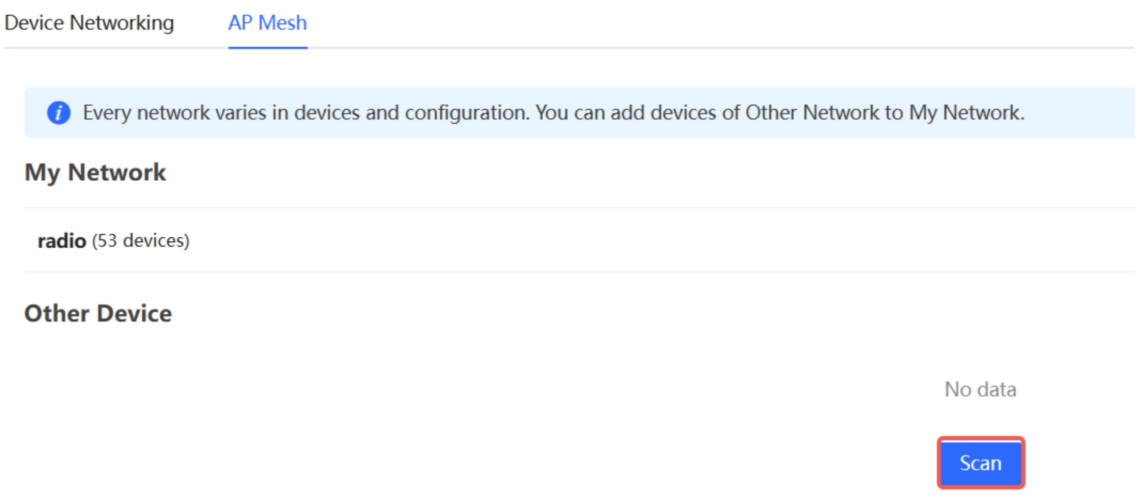
(1) Power on the new AP and place it near the AP or EGW router on the target network.

(2) Log in to the web interface of a device on the target network. In SON mode, click **+Discover Devices** in the upper right corner of the **Physical Topology** page to scan the APs in other networks not connected with Ethernet cables.



Last Updated: 2023-12-15 16:58:23

(3) On the **AP Mesh** page, click **Scan** to scan devices that are not connected to the network via an Ethernet cable.



Device Networking AP Mesh

Every network varies in devices and configuration. You can add devices of Other Network to My Network.

My Network

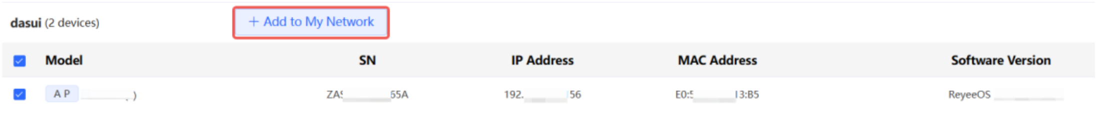
radio (53 devices)

Other Device

No data

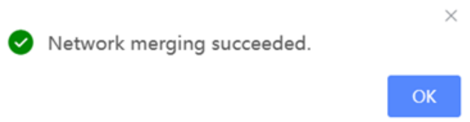
Scan

(4) Select the APs to be added and click **Add to My Network**. Up to eight APs can be added at a time. Wait until the mesh process finishes.



dasui (2 devices) + Add to My Network

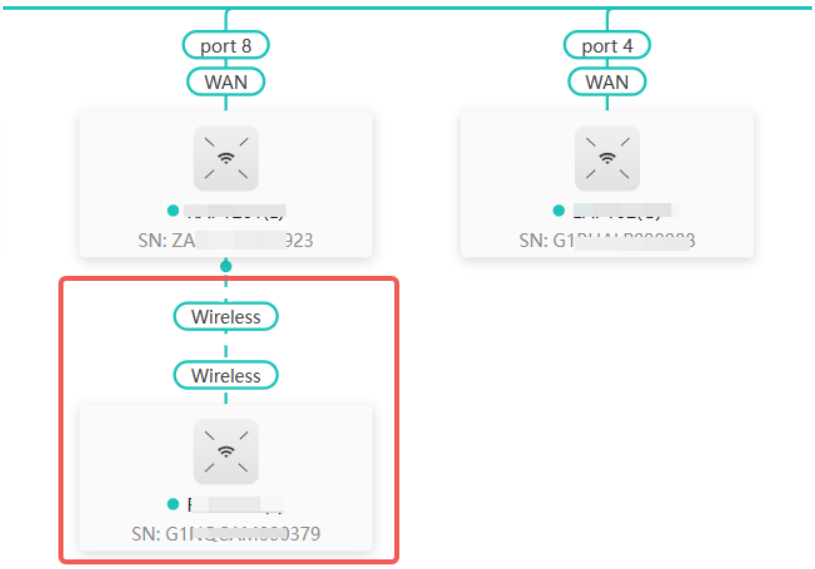
☑	Model	SN	IP Address	MAC Address	Software Version
☑	AP [redacted])	ZA[redacted]55A	192.[redacted]56	E0:[redacted]13:B5	ReyeeOS [redacted]



Network merging succeeded.

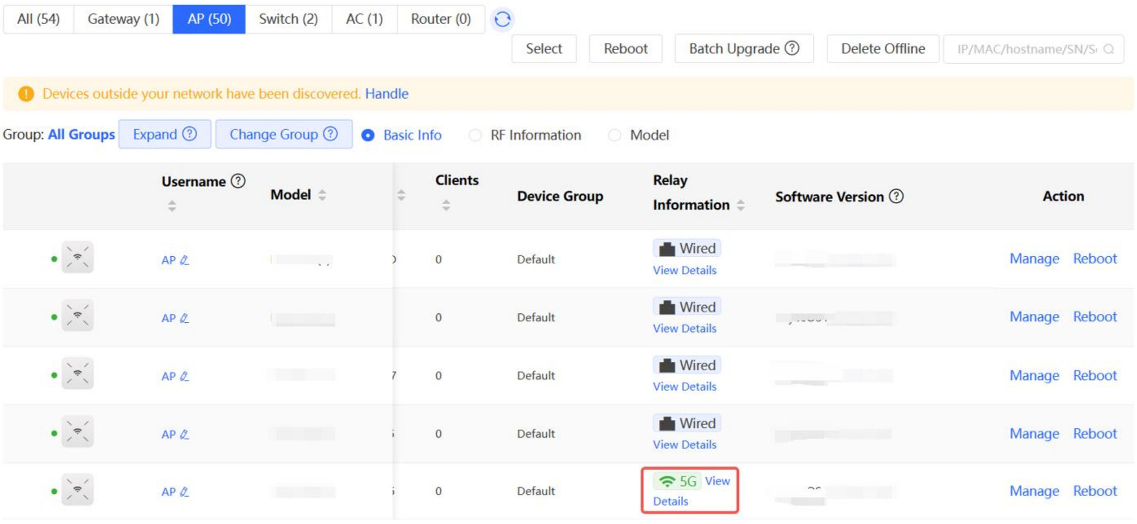
OK

(5) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.



(6) Power off the new AP and install it to the planned location.

(7) Log in to the web interface of a device on the target network. In SON mode, choose **Devices** > **AP**. Make sure that the new AP is online and the icon 5G appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.


All (54) | Gateway (1) | AP (50) | Switch (2) | AC (1) | Router (0)

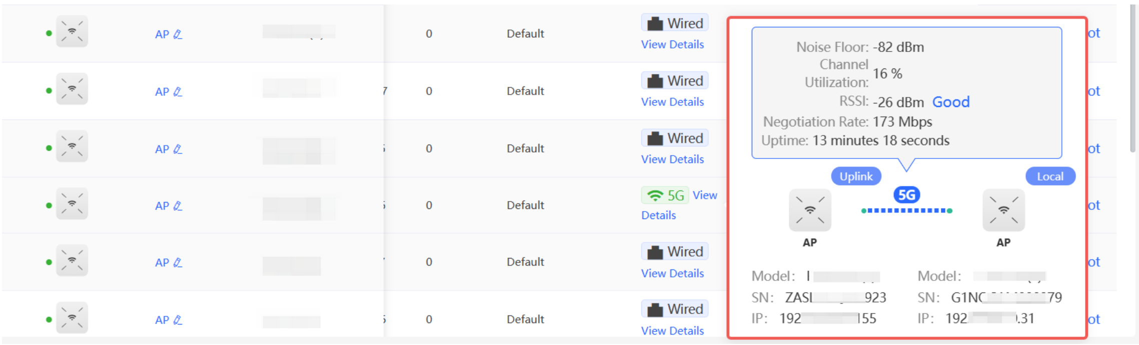
Select | Reboot | Batch Upgrade ⓘ | Delete Offline | IP/MAC/hostname/SN/S

Devices outside your network have been discovered. Handle

Group: All Groups Expand ⓘ Change Group ⓘ ● Basic Info ○ RF Information ○ Model

	Username ⓘ	Model		Clients	Device Group	Relay Information	Software Version ⓘ	Action
●	AP			0	Default	Wired View Details		Manage Reboot
●	AP			0	Default	Wired View Details		Manage Reboot
●	AP			0	Default	Wired View Details		Manage Reboot
●	AP			0	Default	Wired View Details		Manage Reboot
●	AP			0	Default	5G View Details		Manage Reboot

(8) Click **View Details** next to the 5G icon to obtain information about the uplink device and RSSI.


	Username	Model	Clients	Device Group	Relay Information
●	AP		0	Default	Wired View Details
●	AP		0	Default	Wired View Details
●	AP		0	Default	Wired View Details
●	AP		0	Default	5G View Details
●	AP		0	Default	Wired View Details
●	AP		0	Default	Wired View Details

Noise Floor: -82 dBm
Channel Utilization: 16 %
RSSI: -26 dBm Good
Negotiation Rate: 173 Mbps
Uptime: 13 minutes 18 seconds

Model: I
SN: ZASI 923
IP: 192 155

Model:
SN: G1NC 79
IP: 192 .31

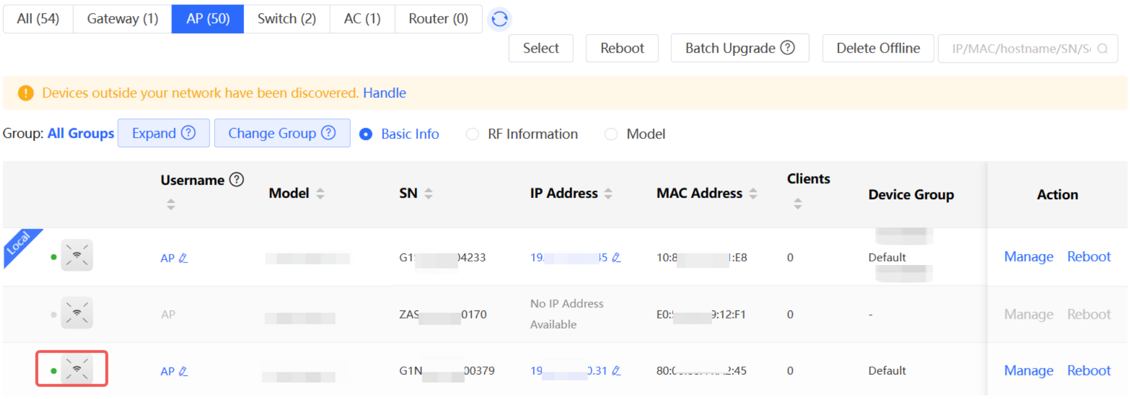
5. Wired Pairing

Caution

- The uplink device can be an AP, EG router, or EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the live network is enabled with AP Mesh.

(1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. The Mesh process takes one to three minutes. When the system status LED is steady on, it indicates that the Mesh process finishes.

(2) Log in to the web interface of a device on the target network. In SON mode, choose **Devices** and make sure that the new AP is online.



All (54) | Gateway (1) | AP (50) | Switch (2) | AC (1) | Router (0)

Select | Reboot | Batch Upgrade ⓘ | Delete Offline | IP/MAC/hostname/SN/S

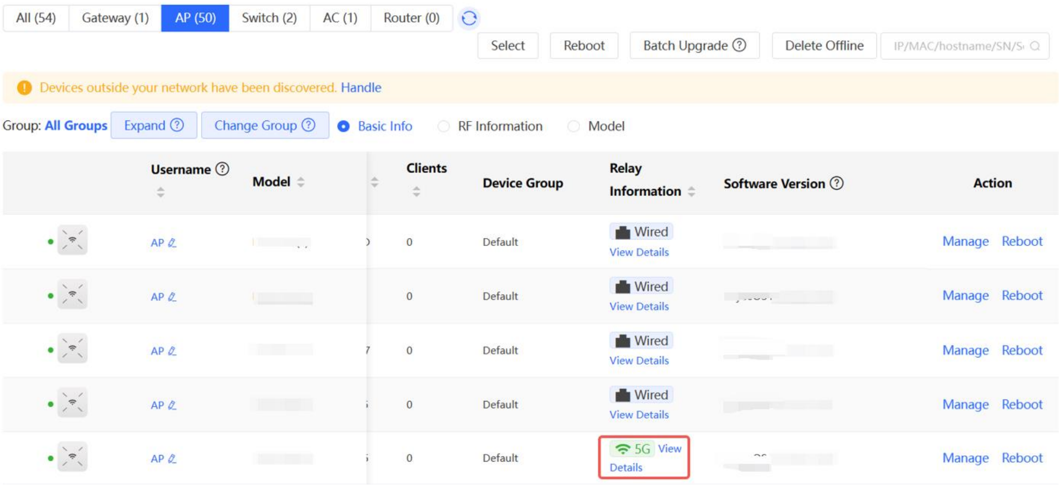
Devices outside your network have been discovered. Handle

Group: All Groups Expand ⓘ Change Group ⓘ ● Basic Info ○ RF Information ○ Model

	Username ⓘ	Model	SN	IP Address	MAC Address	Clients	Device Group	Action
Local	AP	[redacted]	G1[redacted]04233	19[redacted]5	10:8[redacted]:E8	0	Default	Manage Reboot
	AP	[redacted]	ZAS[redacted]0170	No IP Address Available	E0:[redacted]:12:F1	0	-	Manage Reboot
	AP	[redacted]	G1N[redacted]00379	19[redacted].31	80:C[redacted]:45	0	Default	Manage Reboot

(3) Unplug the Ethernet cable, power off the new AP, and install it to a planned location.

(4) Log in to the web interface of a device on the target network. In SON mode, choose **Devices** > **AP**. Make sure that the new AP is online and the icon 5G appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



All (54) | Gateway (1) | AP (50) | Switch (2) | AC (1) | Router (0)

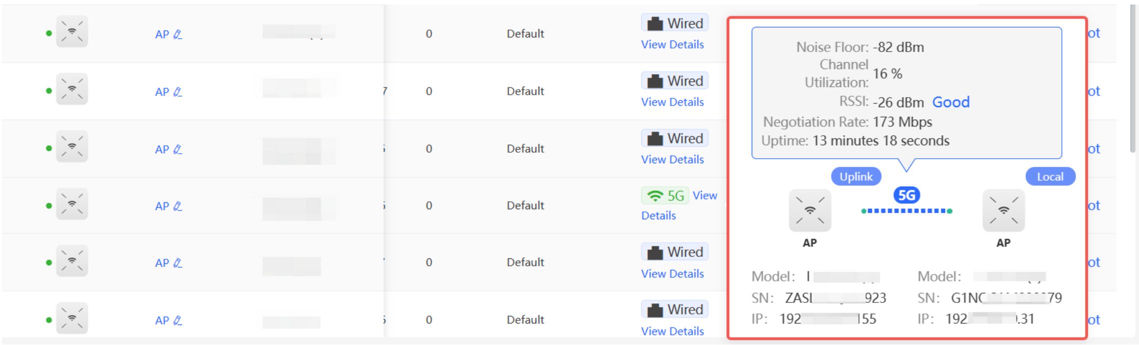
Select | Reboot | Batch Upgrade ⓘ | Delete Offline | IP/MAC/hostname/SN/S

Devices outside your network have been discovered. Handle

Group: All Groups Expand ⓘ Change Group ⓘ ● Basic Info ○ RF Information ○ Model

Username ⓘ	Model	Clients	Device Group	Relay Information	Software Version ⓘ	Action
AP	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
AP	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
AP	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
AP	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
AP	[redacted]	0	Default	5G View Details	[redacted]	Manage Reboot

(5) Click **View Details** next to the 5G icon to obtain information about the uplink device and RSSI.



AP	[redacted]	0	Default	Wired View Details
AP	[redacted]	0	Default	Wired View Details
AP	[redacted]	0	Default	Wired View Details
AP	[redacted]	0	Default	5G View Details
AP	[redacted]	0	Default	Wired View Details
AP	[redacted]	0	Default	Wired View Details

Noise Floor: -82 dBm
Channel Utilization: 16 %
RSSI: -26 dBm Good
Negotiation Rate: 173 Mbps
Uptime: 13 minutes 18 seconds

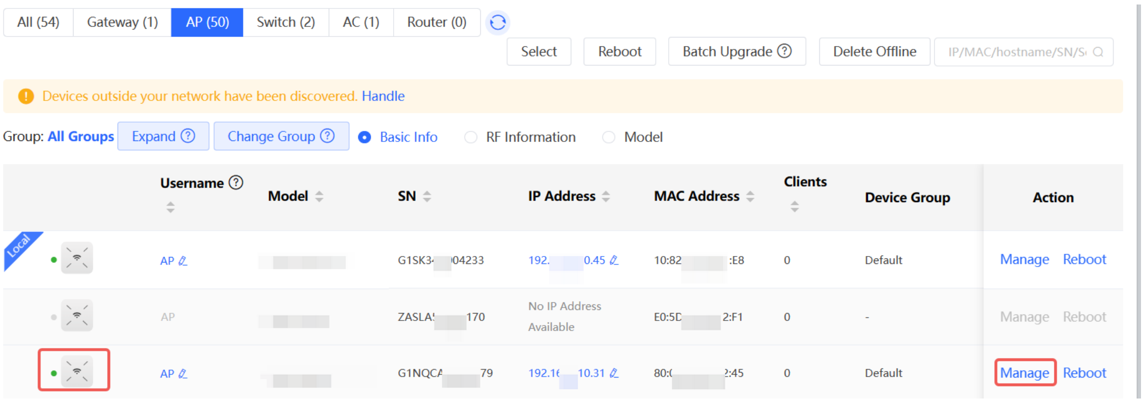
Model: [redacted]
SN: ZASI[redacted]923
IP: 192[redacted]155

Model: [redacted]
SN: G1NC[redacted]79
IP: 192[redacted].31

6. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through Mesh pairing, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

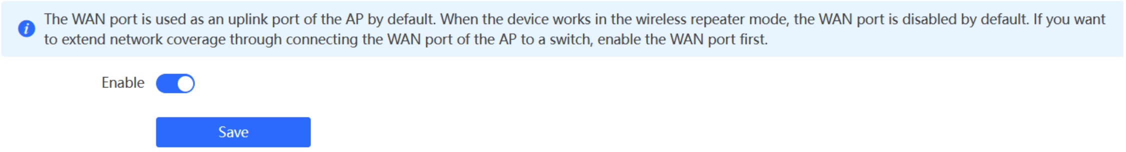
(1) Log in to the web interface of the network project. Choose **Network-Wide** > **Devices** > **AP**, and click **Manage** next to a device in the AP list.



Devices outside your network have been discovered. Handle

	Username ⓘ	Model	SN	IP Address	MAC Address	Clients	Device Group	Action
●	AP	[redacted]	G1SK3[redacted]04233	192.[redacted]0.45	10:82[redacted]:E8	0	Default	Manage Reboot
●	AP	[redacted]	ZASLA[redacted]170	No IP Address Available	E0:5D[redacted]2:F1	0	-	Manage Reboot
●	AP	[redacted]	G1NQC[redacted]79	192.1[redacted]10.31	80:[redacted]:45	0	Default	Manage Reboot

(2) Choose **Config** > **Advanced** > **Enable WAN**, toggle on **Enable**, and click **Save**.



The WAN port is used as an uplink port of the AP by default. When the device works in the wireless repeater mode, the WAN port is disabled by default. If you want to extend network coverage through connecting the WAN port of the AP to a switch, enable the WAN port first.

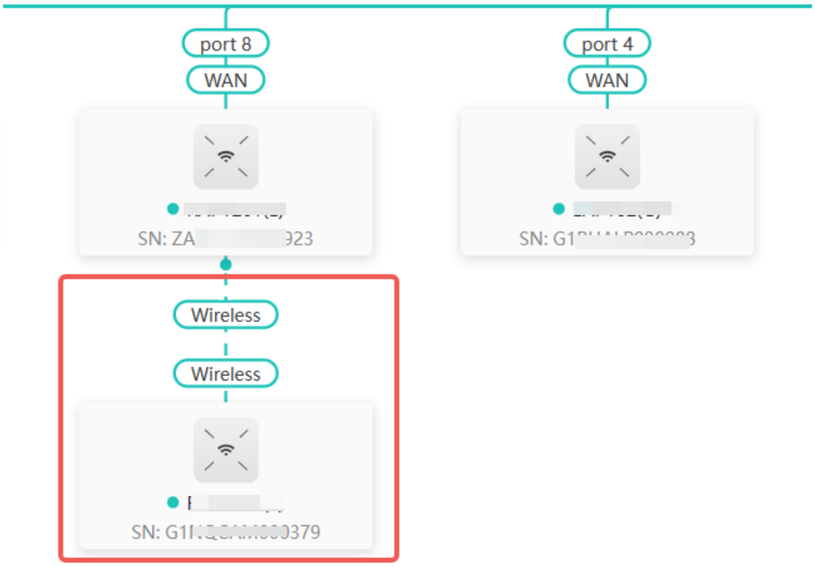
Enable: On

7. Viewing Mesh APs and Mesh Details

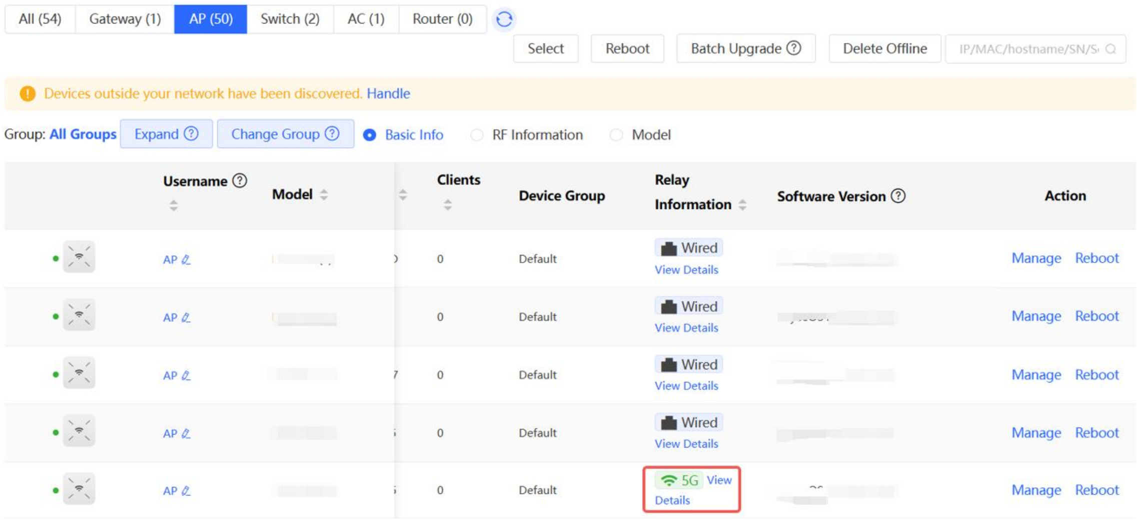
(1) Log in to the web interface of a device on the target network.

(2) View Mesh APs.

- Method 1: In SON mode, check the topology on the **Physical Topology** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.



- Method 2: In SON mode, choose **Devices** > **AP**. If the icon 5G appears in the **Relay Information** column, the corresponding AP is a Mesh AP.



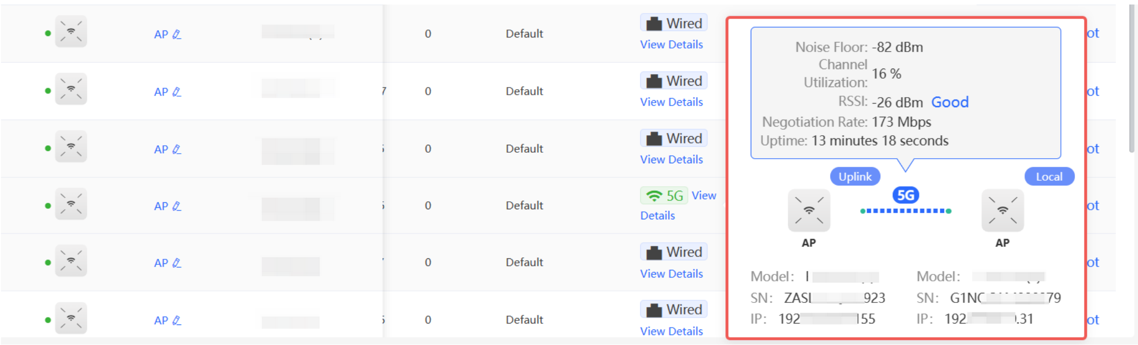
Devices outside your network have been discovered. Handle

Group: **All Groups** Expand Change Group ● Basic Info ○ RF Information ○ Model

	Username	Model		Clients	Device Group	Relay Information	Software Version	Action
●	AP	[redacted]	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
●	AP	[redacted]	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
●	AP	[redacted]	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
●	AP	[redacted]	[redacted]	0	Default	Wired View Details	[redacted]	Manage Reboot
●	AP	[redacted]	[redacted]	0	Default	5G View Details	[redacted]	Manage Reboot

(3) View Mesh details.

In SON mode, choose **Devices** > **AP**. Select the target AP, and click **View Details** in the **Relay Information** column to view the Mesh details.



●	AP	[redacted]	0	Default	Wired View Details	ot
●	AP	[redacted]	0	Default	Wired View Details	ot
●	AP	[redacted]	0	Default	Wired View Details	ot
●	AP	[redacted]	0	Default	5G View Details	ot
●	AP	[redacted]	0	Default	Wired View Details	ot
●	AP	[redacted]	0	Default	Wired View Details	ot

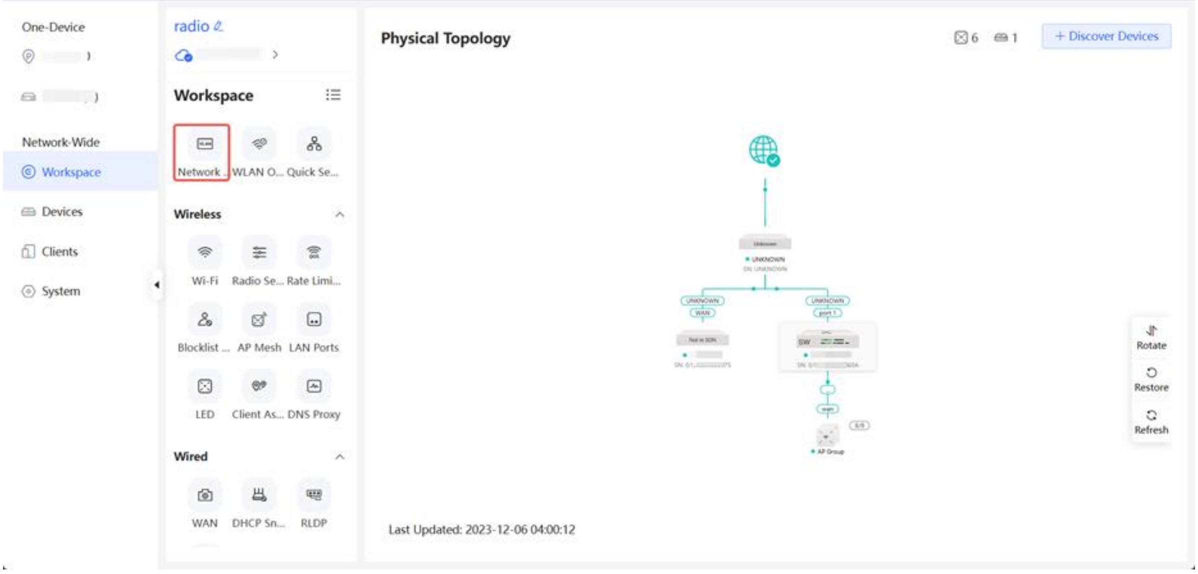
Noise Floor: -82 dBm
Channel Utilization: 16 %
RSSI: -26 dBm Good
Negotiation Rate: 173 Mbps
Uptime: 13 minutes 18 seconds

Model: [redacted]
SN: ZASL[redacted]923
IP: 192[redacted]155

Model: [redacted]
SN: G1NC[redacted]79
IP: 192[redacted].31

3.3 Configuring VLANs

Choose **Network-Wide** > **Workspace** > **Network Planning**.

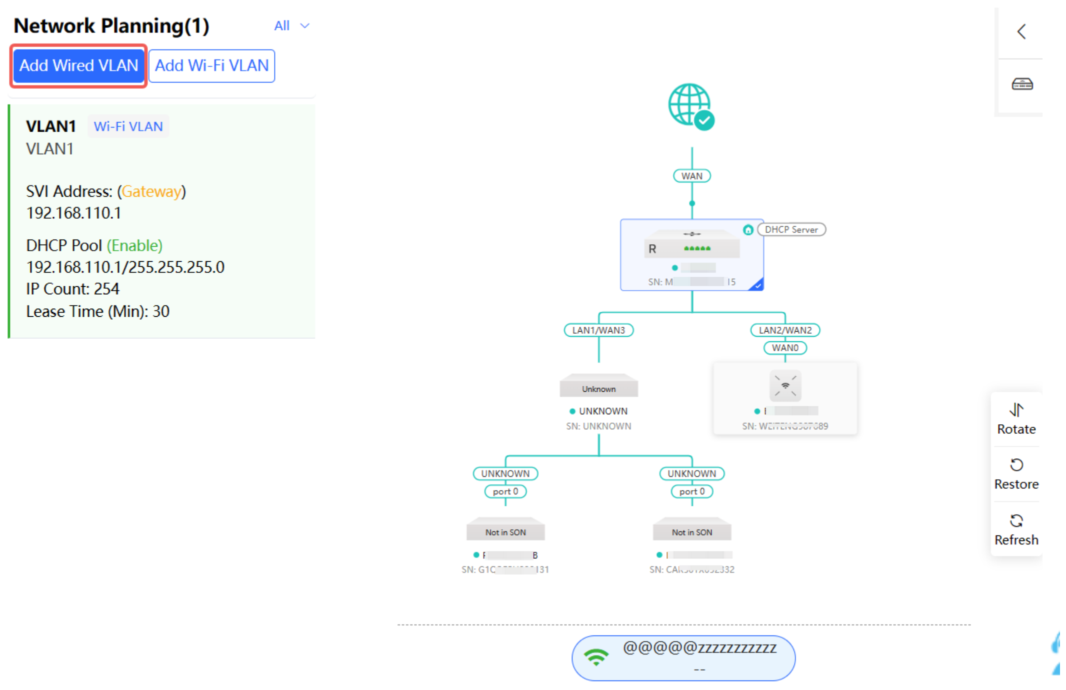


Last Updated: 2023-12-06 04:00:12

3.3.1 Configuring a Wired VLAN

Choose **Network-Wide** > **Workspace** > **Network Planning**.

On the **Network Planning** page, click **Add Wired VLAN**.



Network Planning(1) All

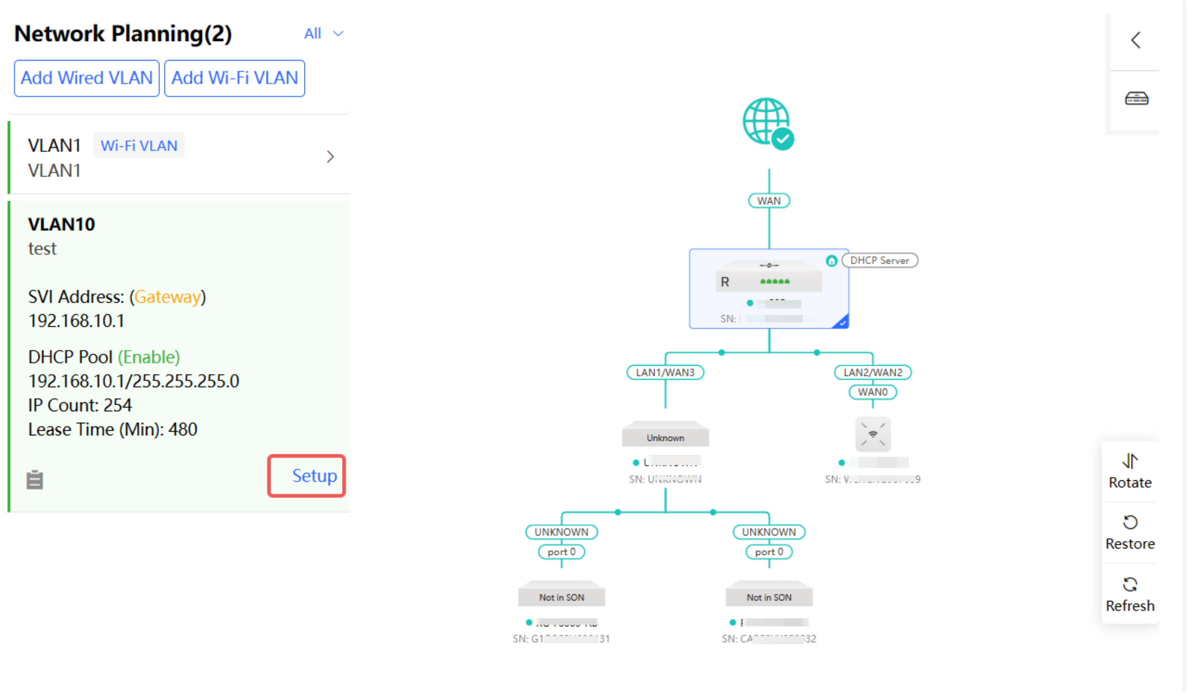
Add Wired VLAN Add Wi-Fi VLAN

VLAN1 Wi-Fi VLAN
VLAN1

SVI Address: (Gateway)
192.168.110.1

DHCP Pool (Enable)
192.168.110.1/255.255.255.0
IP Count: 254
Lease Time (Min): 30

Alternatively, you can select an existing wired VLAN and click **Setup** to edit the VLAN.



Network Planning(2) All

Add Wired VLAN Add Wi-Fi VLAN

VLAN1 Wi-Fi VLAN
VLAN1

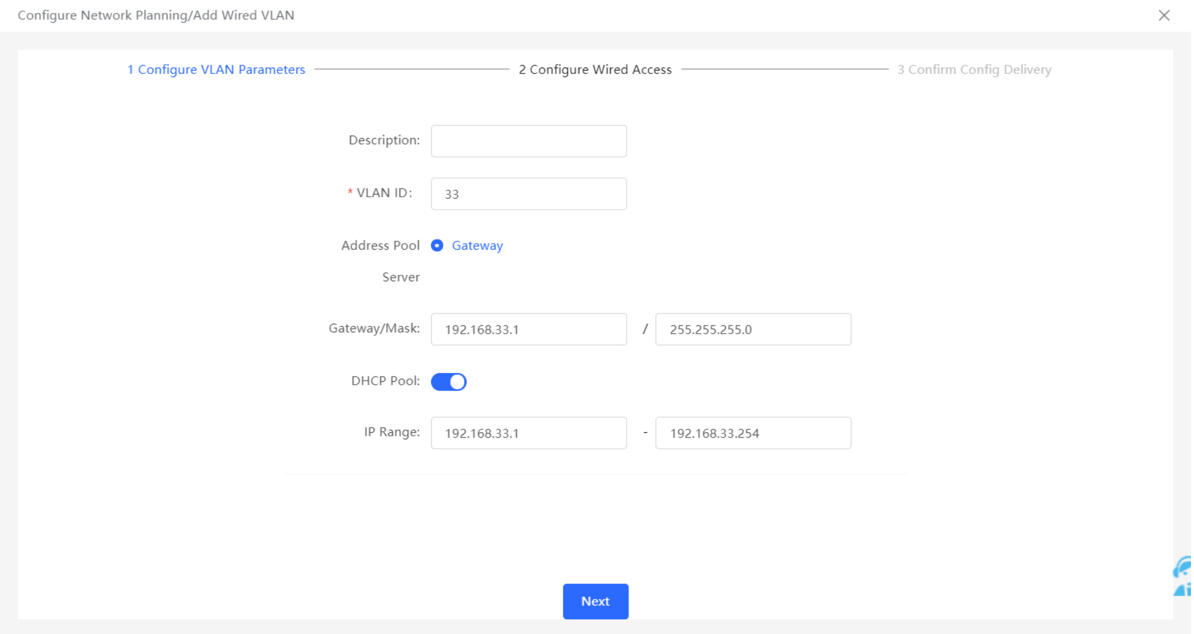
VLAN10
test

SVI Address: (Gateway)
192.168.10.1

DHCP Pool (Enable)
192.168.10.1/255.255.255.0
IP Count: 254
Lease Time (Min): 480

Setup

(1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists on the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



Configure Network Planning/Add Wired VLAN

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

Description:

* VLAN ID: 33

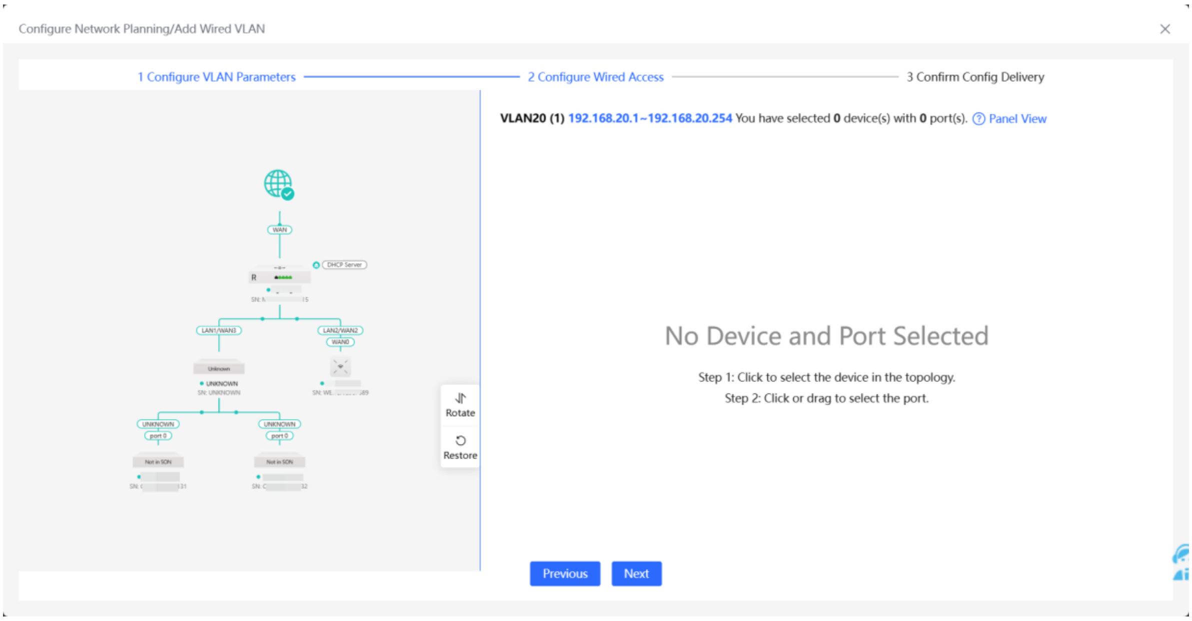
Address Pool Server: ● Gateway

Gateway/Mask: 192.168.33.1 / 255.255.255.0

DHCP Pool: On

IP Range: 192.168.33.1 - 192.168.33.254

(2) Select the target switch in the topology and all member ports in the VLAN, and click **Next**.



Configure Network Planning/Add Wired VLAN

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

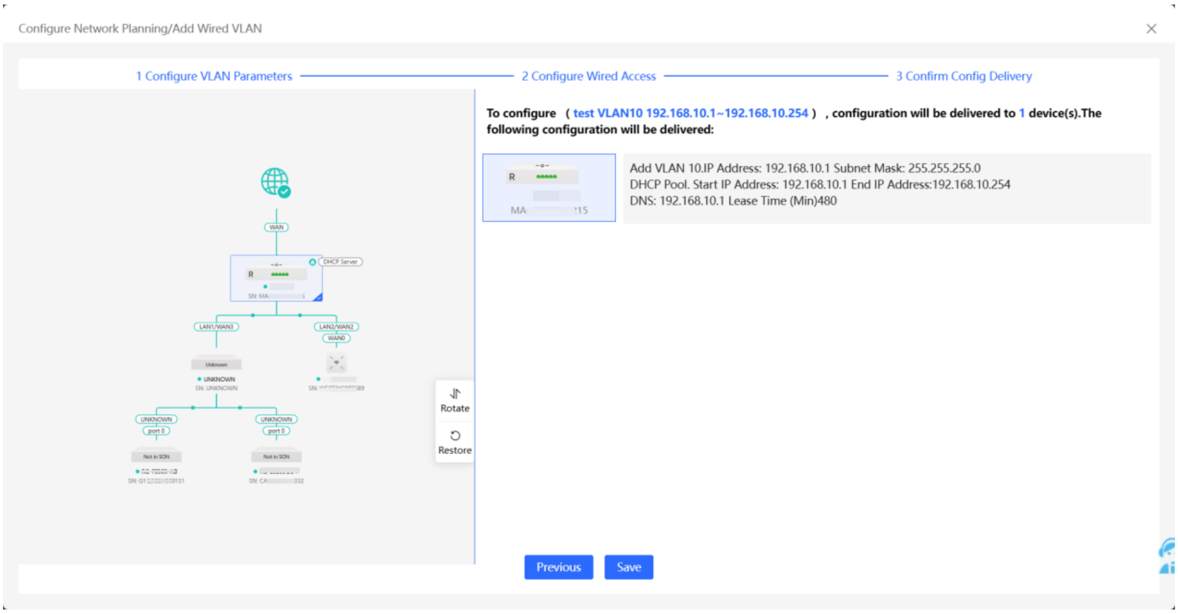
VLAN20 (1) 192.168.20.1~192.168.20.254 You have selected **0** device(s) with **0** port(s). ⓘ Panel View

No Device and Port Selected

Step 1: Click to select the device in the topology.

Step 2: Click or drag to select the port.

(3) Confirm the configurations and click **Save**. The configurations will take effect in a few minutes.



Configure Network Planning/Add Wired VLAN

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

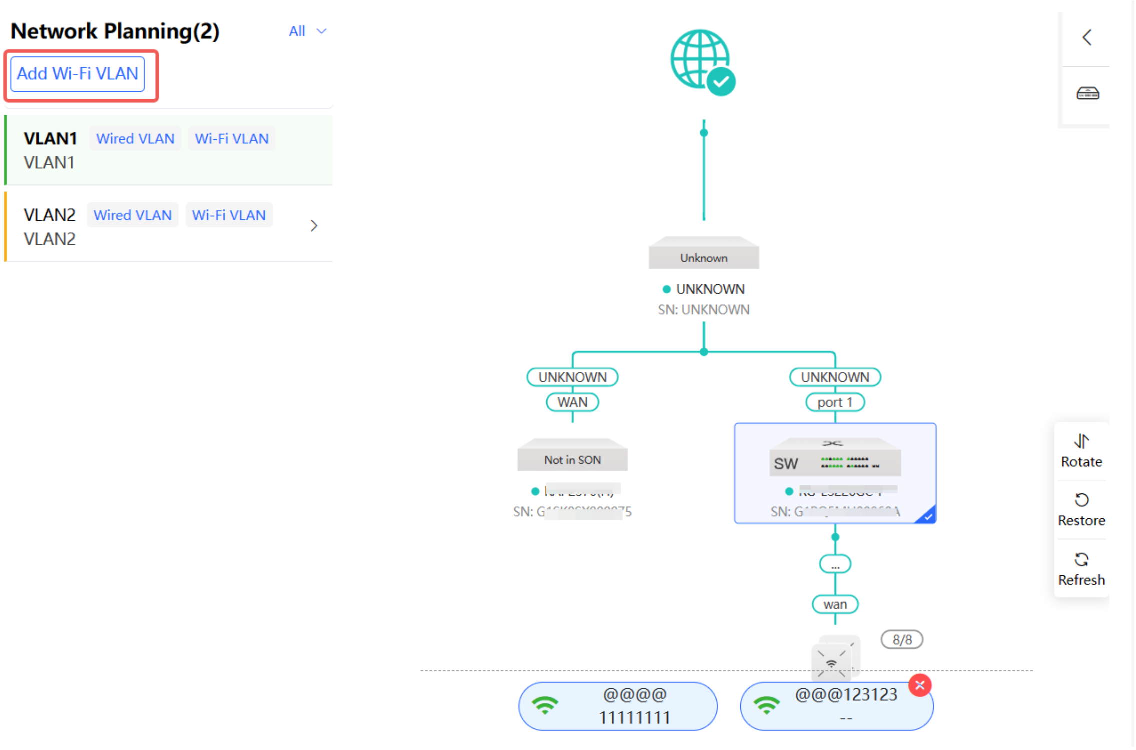
To configure （test VLAN10 192.168.10.1~192.168.10.254）, configuration will be delivered to 1 device(s).The following configuration will be delivered:

Add VLAN 10.IP Address: 192.168.10.1 Subnet Mask: 255.255.255.0
DHCP Pool. Start IP Address: 192.168.10.1 End IP Address:192.168.10.254
DNS: 192.168.10.1 Lease Time (Min)480

3.3.2 Configuring a Wi-Fi VLAN

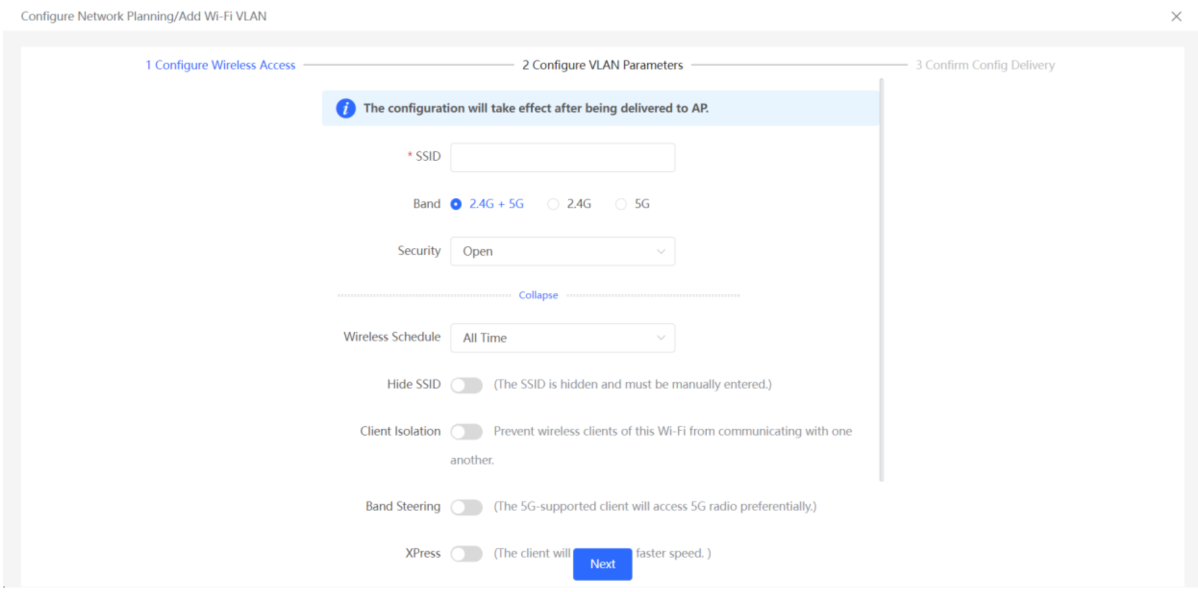
Choose **Network-Wide** > **Workspace** > **Network Planning**.

On the **Network Planning** page, click **Add Wi-Fi LAN**.



Alternatively, you can select an existing wireless VLAN and click **Setup** to edit the VLAN.

(1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.



Configure Network Planning/Add Wi-Fi VLAN

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

The configuration will take effect after being delivered to AP.

* SSID

Band ● 2.4G + 5G ○ 2.4G ○ 5G

Security: Open

Wireless Schedule: All Time

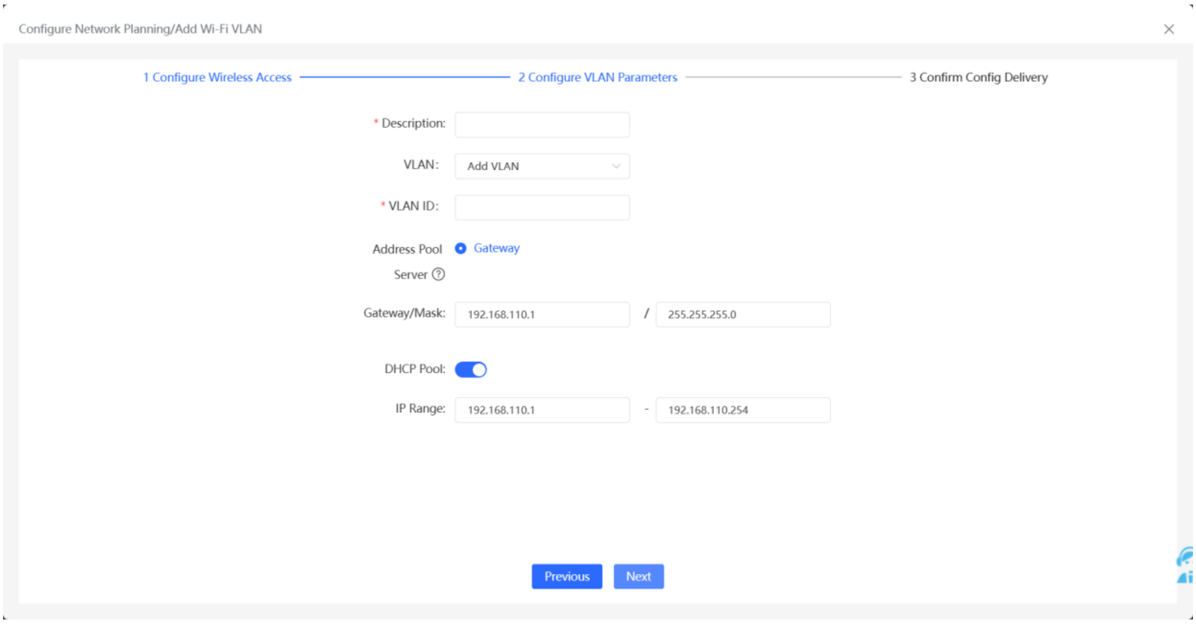
Hide SSID (The SSID is hidden and must be manually entered.)

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 faster speed.)

(2) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists on the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



Configure Network Planning/Add Wi-Fi VLAN

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

* Description:

VLAN: Add VLAN

* VLAN ID:

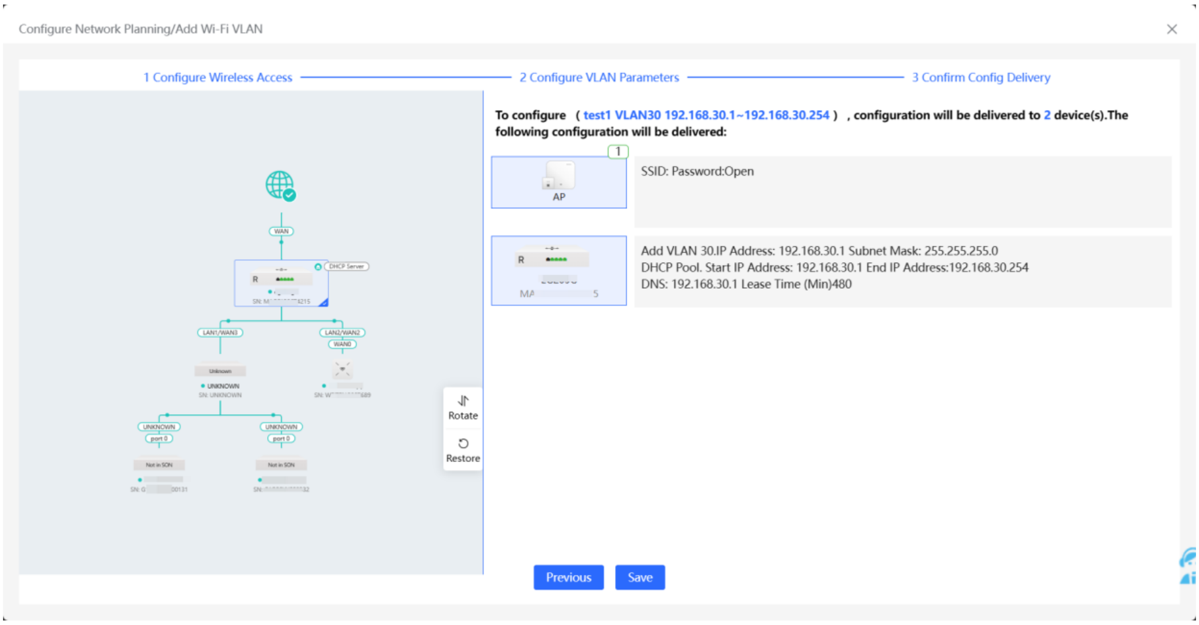
Address Pool Server ⓘ ● Gateway

Gateway/Mask: 192.168.110.1 / 255.255.255.0

DHCP Pool: On

IP Range: 192.168.110.1 - 192.168.110.254

(3) Confirm the delivered configurations and click **Save**. The configurations will take effect in a few minutes.



Configure Network Planning/Add Wi-Fi VLAN

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

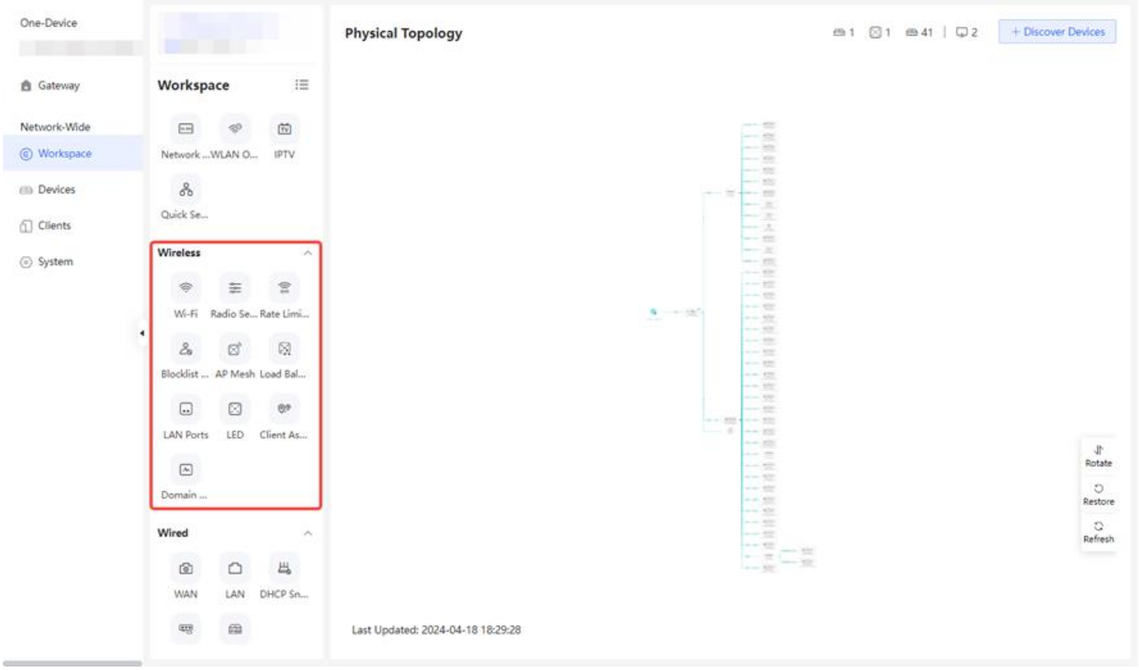
To configure （test1 VLAN30 192.168.30.1~192.168.30.254）, configuration will be delivered to 2 device(s).The following configuration will be delivered:

AP: SSID: Password:Open

Add VLAN 30.IP Address: 192.168.30.1 Subnet Mask: 255.255.255.0
DHCP Pool. Start IP Address: 192.168.30.1 End IP Address:192.168.30.254
DNS: 192.168.30.1 Lease Time (Min)480

3.4 Network-wide Wireless Management

Choose **Network-Wide** > **Workspace** > **Wireless**.



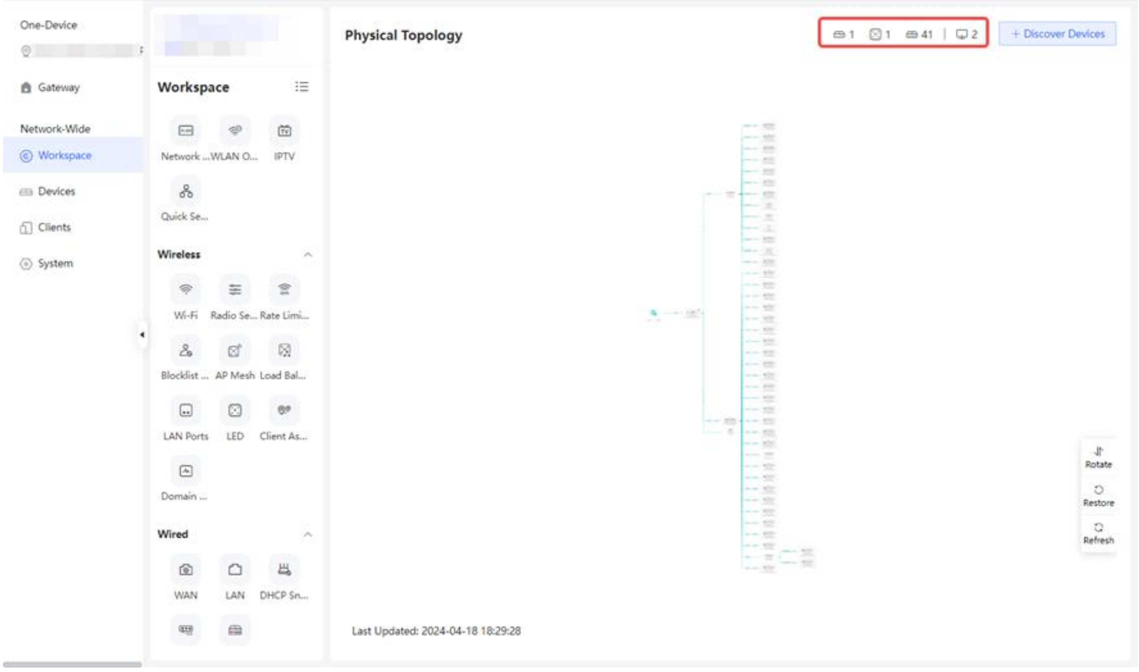
Last Updated: 2024-04-18 18:29:28

The functions supported by Network-wide Wireless Management depend on the APs on the network. Detailed information on the supported functions can be found in the Web-based Configuration Guide of RG-RAP and RG-EAP devices. For example, if the software version of the AP device is OS 2.280, the functions supported by Network-wide Wireless Management can be referenced in the RG-RAP and RG-EAP Web-based Configuration Guide for OS 2.280 version.

3.5 Device Management

View all devices on the current network. You can configure and manage the devices simply by logging into one device on the network. The methods to access device management are as follows:

Method 1: Click the device icon in the top right corner of the **Physical Topology** to switch to the device list view.



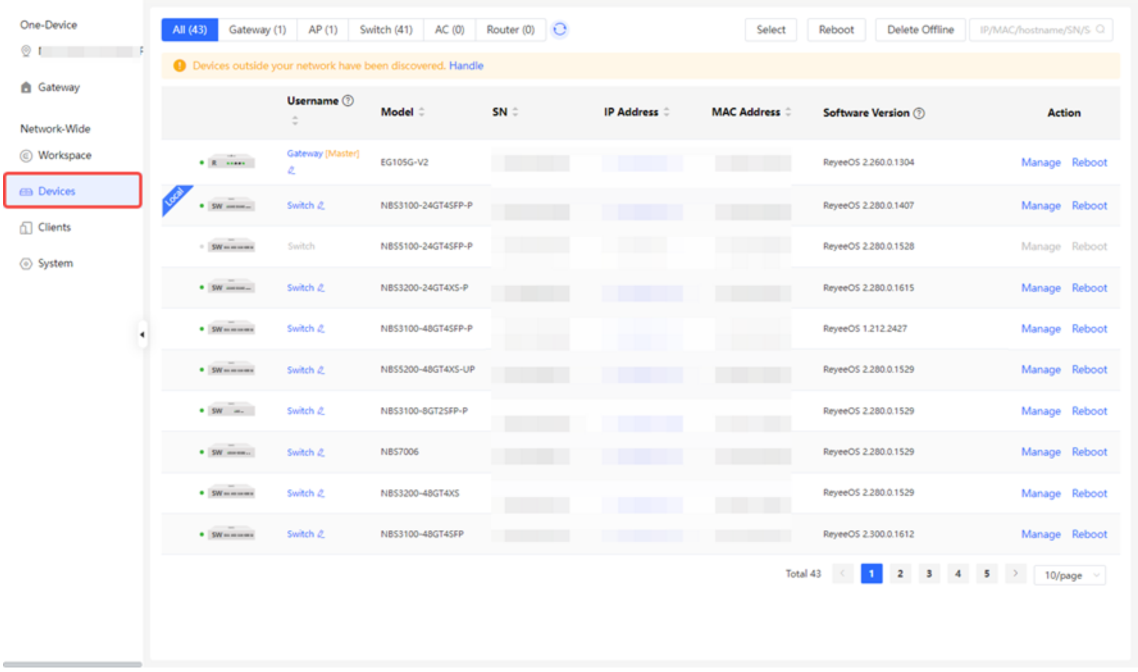
Method 2: Choose **Network-Wide** > Devices

Click Handle to add a device to the current network.

Click Manage to configure a specific device.

Click Reboot to restart a specific device.

Click Select to select offline devices. Then, click Delete Offline. The selected devices will be removed from the list and network topology.



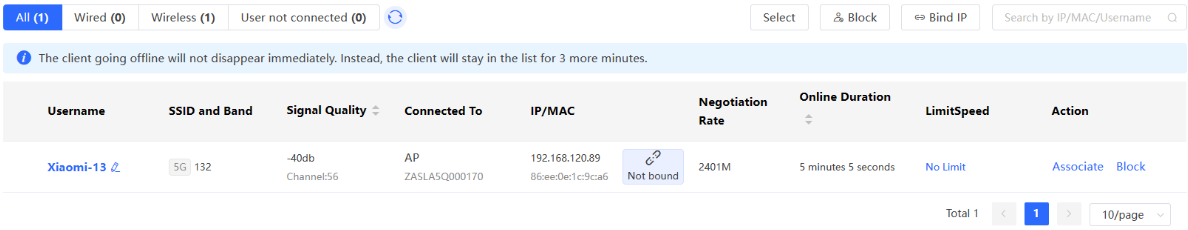
Devices outside your network have been discovered. Handle

Username	Model	SN	IP Address	MAC Address	Software Version	Action
Gateway [Master]	EG105G-V2	[redacted]	[redacted]	[redacted]	ReyeeOS 2.260.0.1304	Manage Reboot
Switch	NBS3100-24GT4SFP-P	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1407	Manage Reboot
Switch	NBS5100-24GT4SFP-P	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1528	Manage Reboot
Switch	NBS3200-24GT4XS-P	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1615	Manage Reboot
Switch	NBS3100-48GT4SFP-P	[redacted]	[redacted]	[redacted]	ReyeeOS 1.212.2427	Manage Reboot
Switch	NBS5200-48GT4XS-UP	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1529	Manage Reboot
Switch	NBS3100-8GT2SFP-P	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1529	Manage Reboot
Switch	NBS7006	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1529	Manage Reboot
Switch	NBS3200-48GT4XS	[redacted]	[redacted]	[redacted]	ReyeeOS 2.280.0.1529	Manage Reboot
Switch	NBS3100-48GT4SFP	[redacted]	[redacted]	[redacted]	ReyeeOS 2.300.0.1612	Manage Reboot

3.6 Online Client Management

Choose **Network-Wide** > **Clients**.

The client list displays wired, wireless, and users not connected on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Not bound	2401M	5 minutes 5 seconds	No Limit	Associate Block

- Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.
- Click a button in the **Action** column to perform the corresponding operation on the online client.
  - Wired: Only access control can be configured.
  - Wireless: Access control, associate, and block can be configured.

Note

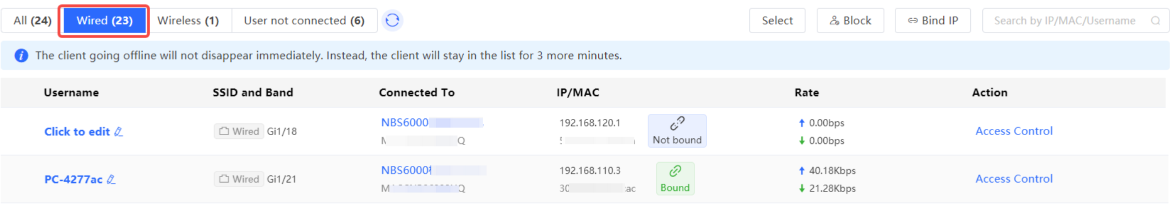
IP binding and access control are supported only in router mode.

Table 3-1 Online Client Management Configuration Parameters

Parameter	Description
Username	Name of the connected client.
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.
Signal Quality	The Wi-Fi signal strength of the client and the associated channel. **Note** This information is displayed only in the wireless online client list.
Connected To	Indicates wired or wireless connection, the associated device and SN.
IP/MAC	Indicates the IP address and MAC address of the client.
Negotiated Rate	The uplink data rate and downlink data rate of the client. **Note** This information is displayed only in the wireless online client list.
Online Duration	Client access duration. **Note** This information is displayed only in the wireless online client list.
LimitSpeed	Implement wireless speed limiting for clients to prevent certain clients from consuming large amounts of bandwidth resources. For details, see 3.6.4 Configuring Client Rate Limiting. **Note** This information is displayed only in the wireless online client list.
Action	You can click the corresponding button to perform access control, association, and block operations on online clients.

Wired Clients

Click the **Wired** tab to see details about wired clients.

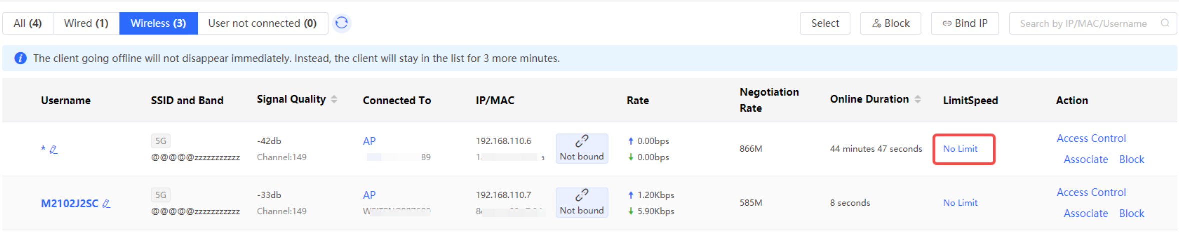


The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Connected To	IP/MAC		Rate	Action
Click to edit	Wired Gi1/18	NBS6000[redacted] N[redacted]Q	192.168.120.1 [redacted]	Not bound	↑ 0.00bps ↓ 0.00bps	Access Control
PC-4277ac	Wired Gi1/21	NBS6000[redacted] M[redacted]Q	192.168.110.3 30[redacted]ac	Bound	↑ 40.18Kbps ↓ 21.28Kbps	Access Control

Wireless Clients

Click the **Wireless** tab to see details about wireless clients.

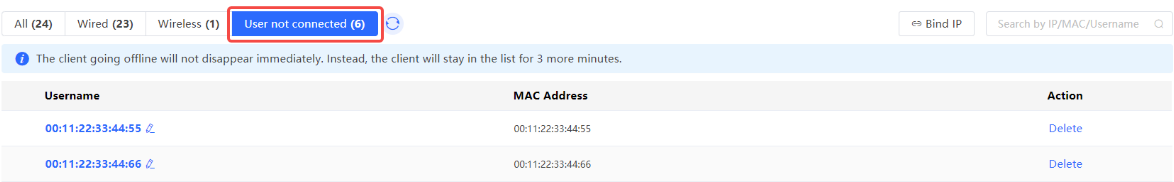


The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Signal Quality	Connected To	IP/MAC		Rate	Negotiation Rate	Online Duration	LimitSpeed	Action
*	5G @@@@@zzzzzzzzzzz	-42db Channel:149	AP [redacted] 89	192.168.110.6 1[redacted]	Not bound	↑ 0.00bps ↓ 0.00bps	866M	44 minutes 47 seconds	No Limit	Access Control Associate Block
M2102J2SC	5G @@@@@zzzzzzzzzzz	-33db Channel:149	AP W[redacted]	192.168.110.7 8[redacted]	Not bound	↑ 1.20Kbps ↓ 5.90Kbps	585M	8 seconds	No Limit	Access Control Associate Block

User not connected

Click the **User not connected tab** to see details about clients waiting to connect. This list includes clients tagged manually or recognized as devices previously connected to the network but not currently listed in device management or online client lists. To remove a client device, click **Delete**.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	MAC Address	Action
00:11:22:33:44:55	00:11:22:33:44:55	Delete
00:11:22:33:44:66	00:11:22:33:44:66	Delete

3.6.1 Configuring Client IP Binding

Note

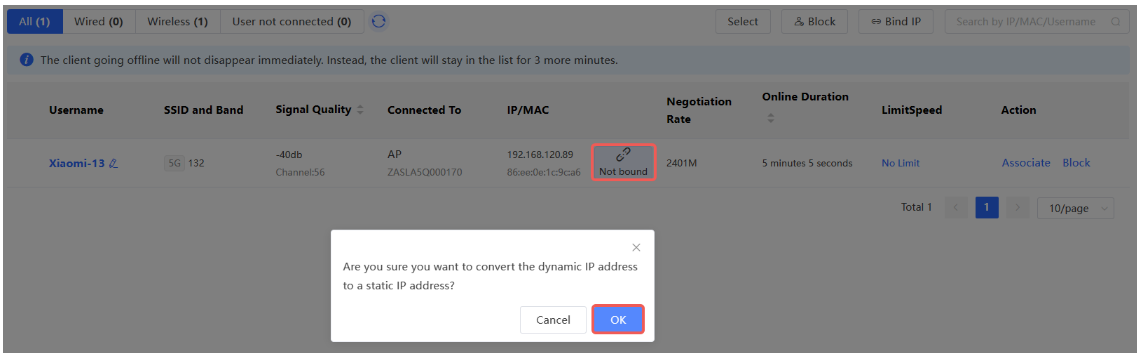
This function is supported only in router mode.

Choose **Network-Wide** > **Clients**.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

- Single client IP address binding

  Select the client to be bound with an IP address in the list, click **Not bound**, and click **OK** in the pop-up box to bind the client to a static IP address.



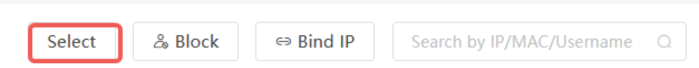
The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Signal Quality	Connected To	IP/MAC		Negotiation Rate	Online Duration	LimitSpeed	Action
Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6	Not bound	2401M	5 minutes 5 seconds	No Limit	Associate Block

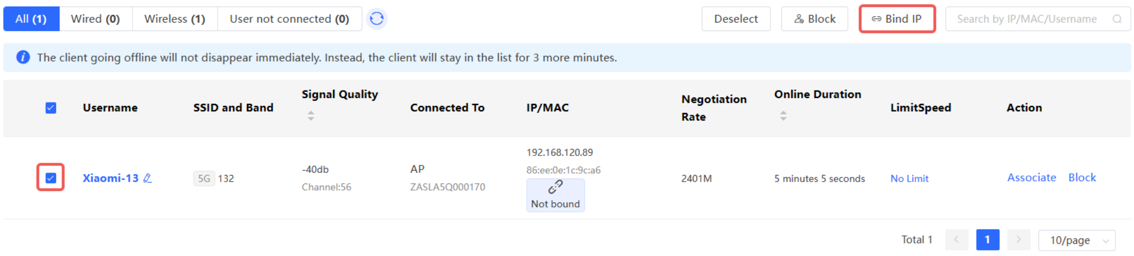
Are you sure you want to convert the dynamic IP address to a static IP address?

- Batch IP binding

  Click **Select**.



Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.



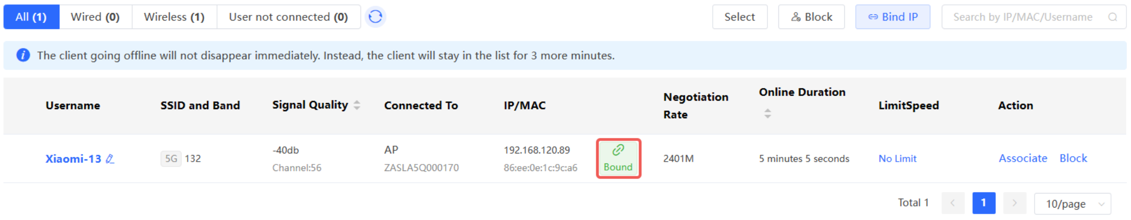
The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

☑	Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
☑	Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Not bound	2401M	5 minutes 5 seconds	No Limit	Associate Block

Total 1 < 1 > 10/page

- Unbind an IP address

Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

Username	SSID and Band	Signal Quality	Connected To	IP/MAC		Negotiation Rate	Online Duration	LimitSpeed	Action
Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6	Bound	2401M	5 minutes 5 seconds	No Limit	Associate Block

Total 1 < 1 > 10/page

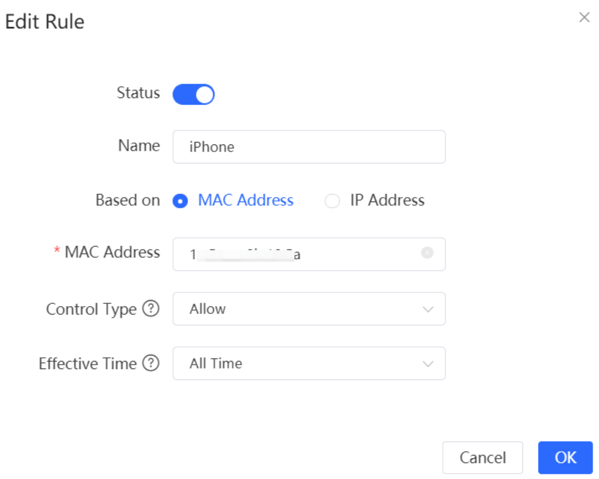
3.6.2 Configuring Client Access Control

Note

This function is supported only in router mode.

Choose **Network-Wide** > **Clients**.

Select a client in the list and click **Access Control** in the **Action** column. You will be redirected to the **Edit Rule** page, where a MAC-based access control rule is automatically generated. The name and MAC address are automatically generated based on the selected client. After selecting the control type and effective time, click **OK** to create an access control rule for the client.



Edit Rule

Status: on

Name: iPhone

Based on: ● MAC Address ○ IP Address

* MAC Address: 1[redacted]a

Control Type ?: Allow

Effective Time ?: All Time

3.6.3 Blocking Clients

Choose **Network-Wide** > **Clients**.

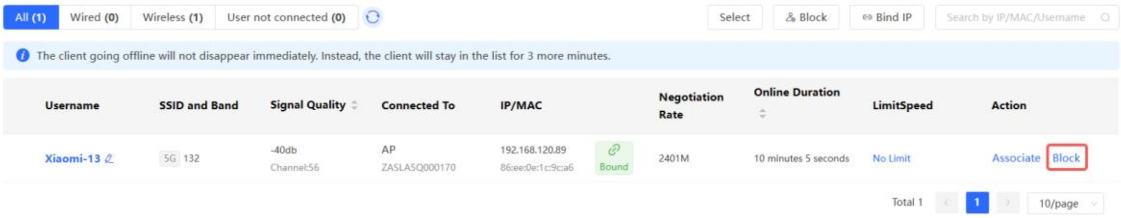
An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

Note

Client block is available only for wireless clients.

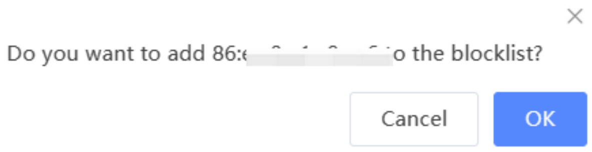
- Block a single client

  Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

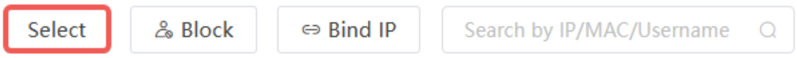
Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Bound	2401M	10 minutes 5 seconds	No Limit	Associate Block



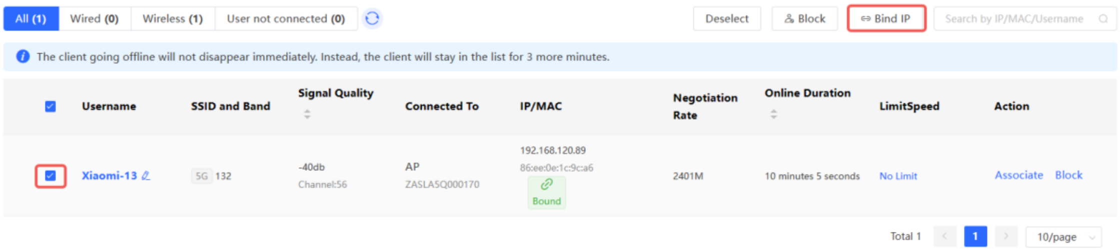
Do you want to add 86:ε[redacted]o the blocklist?

- Batch block clients

  a Click **Select**.



  b Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



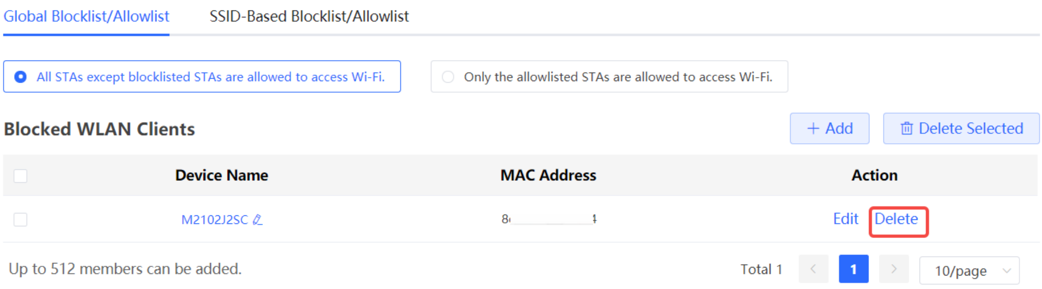
The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

☑	Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
☑	Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Bound	2401M	10 minutes 5 seconds	No Limit	Associate Block

- Cancel block

  Choose **Network-Wide** > **Workspace** > **Wireless** > **Blocklist/Allowlist** > **Global Blocklist/Allowlist.**

  Select the client to be removed from the blocklist in the wireless blocklist and click **Delete**.



● All STAs except blocklisted STAs are allowed to access Wi-Fi.

○ Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

□	Device Name	MAC Address	Action
□	M2102J2SC	8[redacted]4	Edit Delete

Up to 512 members can be added.

3.6.4 Configuring Client Rate Limiting

Choose **Network-Wide** > **Clients** > **Wireless**.

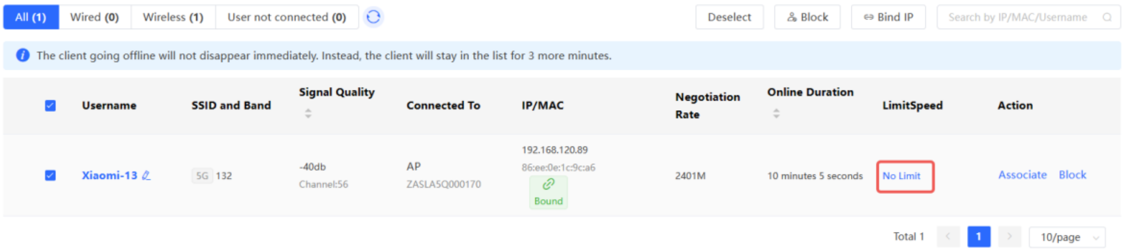
To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

Note

Rate limiting applies only to wireless clients.

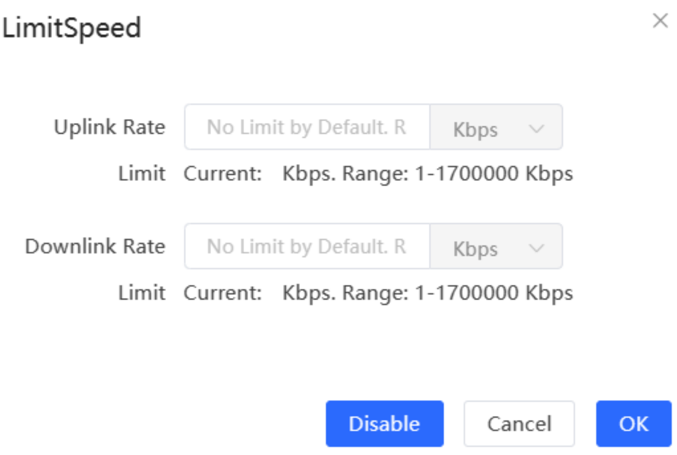
- Configure rate limits for clients

  Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

☑	Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
☑	Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Bound	2401M	10 minutes 5 seconds	No Limit	Associate Block



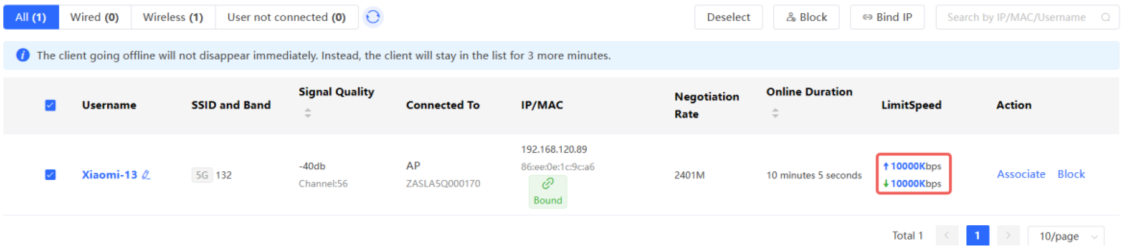
LimitSpeed

Uplink Rate Limit: No Limit by Default. R | Kbps
Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit: No Limit by Default. R | Kbps
Current: Kbps. Range: 1-1700000 Kbps

- Cancel rate limits

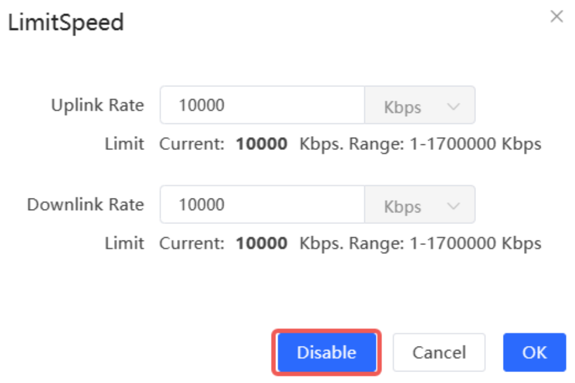
Click the **Wireless** tab, click the **LimitSpeed** column in the table, and click **Disable**.



The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

☑	Username	SSID and Band	Signal Quality	Connected To	IP/MAC	Negotiation Rate	Online Duration	LimitSpeed	Action
☑	Xiaomi-13	5G 132	-40db Channel:56	AP ZASLA5Q000170	192.168.120.89 86:ee:0e:1c:9c:a6 Bound	2401M	10 minutes 5 seconds	↑10000Kbps ↓10000Kbps	Associate Block

Total 1 < 1 > 10/page



LimitSpeed

Uplink Rate 10000 Kbps

Limit Current: **10000** Kbps. Range: 1-1700000 Kbps

Downlink Rate 10000 Kbps

Limit Current: **10000** Kbps. Range: 1-1700000 Kbps

3.7 Firewall Management

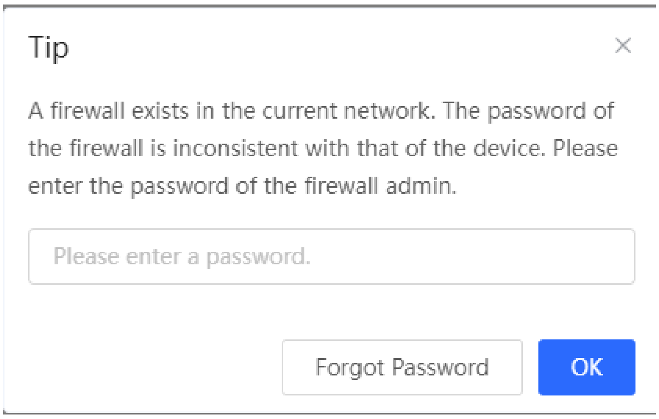
After a firewall is added to the network, you can manage and configure the firewall on the Web management system.

3.7.1 Viewing Firewall Information

You can view the basic information and license of the firewall on the Web management system.

Choose **Network-Wide** > **Network** > **Firewall**.

(1) If the password of the firewall is inconsistent with that of the gateway, please enter the management password of the firewall and click **OK**.

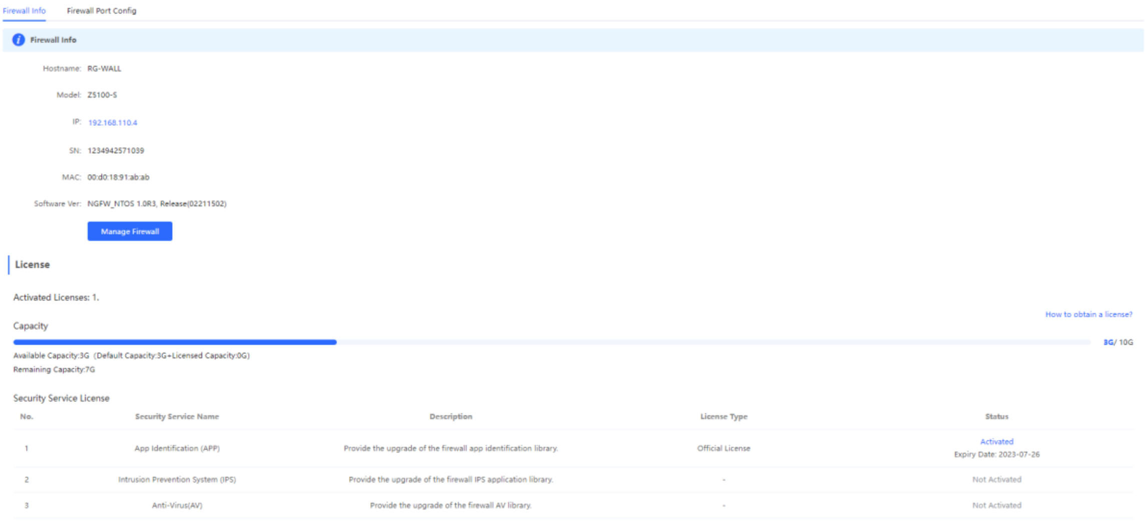


Tip

A firewall exists in the current network. The password of the firewall is inconsistent with that of the device. Please enter the password of the firewall admin.

Please enter a password.

(2) The basic information, capacity, and security service license of the firewall are displayed on the Web management system.



Firewall Info Firewall Port Config

Firewall Info

Hostname: RG-WALL

Model: Z5100-S

IP: 192.168.110.4

SN: 1234942571039

MAC: 00:d0:18:91:ab:ab

Software Ver: NGFW_NTOS 1.0R3, Release(02211502)

Manage Firewall

License

Activated Licenses: 1.

Capacity

How to obtain a license?

3G/ 10G

Available Capacity:3G (Default Capacity:3G+Licensed Capacity:0G)

Remaining Capacity:7G

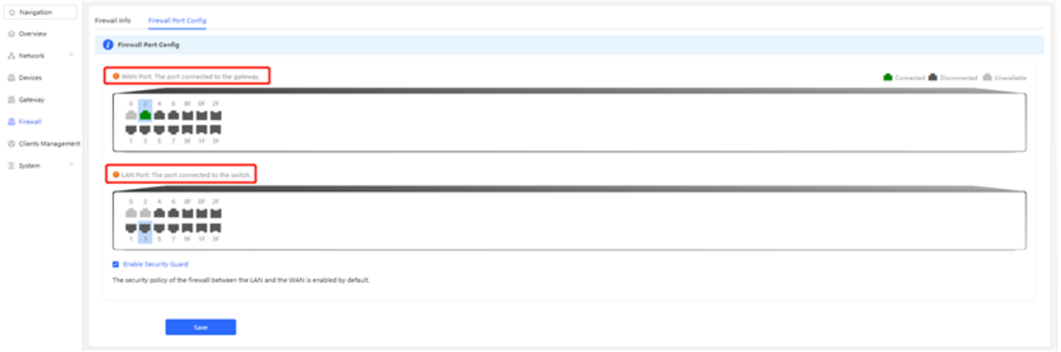
Security Service License

No.	Security Service Name	Description	License Type	Status
1	App Identification (APP)	Provide the upgrade of the firewall app identification library.	Official License	Activated Expiry Date: 2023-07-26
2	Intrusion Prevention System (IPS)	Provide the upgrade of the firewall IPS application library.	-	Not Activated
3	Anti-Virus(AV)	Provide the upgrade of the firewall AV library.	-	Not Activated

Click **Manage Firewall** to go to the Web management interface of the firewall. Configure the security policy and license activation for the firewall. For details, see the Web-based configuration guide of the firewall.

3.7.2 Configuring Firewall Port

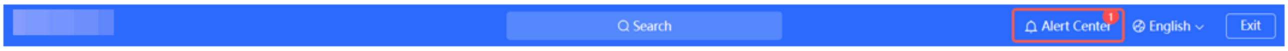
If the firewall is set to transparent mode, the **Firewall Port Config** page appears. You can select the WAN port connected to the gateway or the LAN port connected to the switch and enable **Security Guard**.



The security policy of the firewall between the LAN and the WAN is enabled by default.

3.8 Alerts

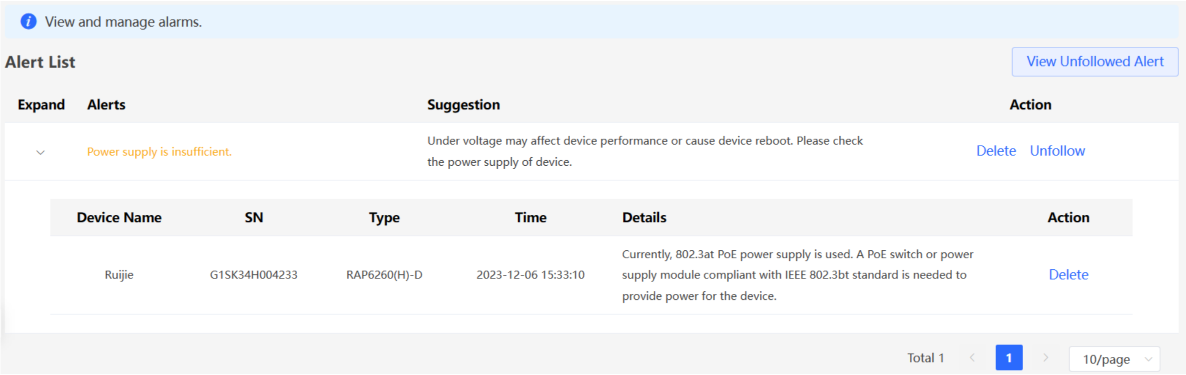
When a network exception occurs, the network overview page will display an alert and provide a suggestion. Click an alert in the **Alert Center** to view the faulty device, problem details, and description. You can troubleshoot the fault based on the suggestion.



The **Alert List** page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

Caution

After unfollowing a specified alert type, you will not discover and process all alerts of this type promptly. Therefore, exercise caution when performing this operation.

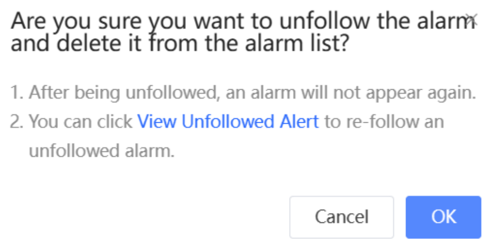


View and manage alarms.

Alert List

Expand	Alerts	Suggestion	Action
⌄	Power supply is insufficient.	Under voltage may affect device performance or cause device reboot. Please check the power supply of device.	Delete Unfollow

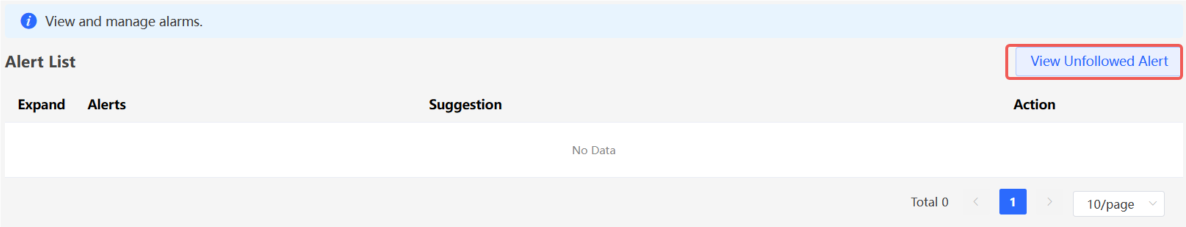
Device Name	SN	Type	Time	Details	Action
Ruijie	G1SK34H004233	RAP6260(H)-D	2023-12-06 15:33:10	Currently, 802.3at PoE power supply is used. A PoE switch or power supply module compliant with IEEE 802.3bt standard is needed to provide power for the device.	Delete



Are you sure you want to unfollow the alarm and delete it from the alarm list?

1. After being unfollowed, an alarm will not appear again.
2. You can click View Unfollowed Alert to re-follow an unfollowed alarm.

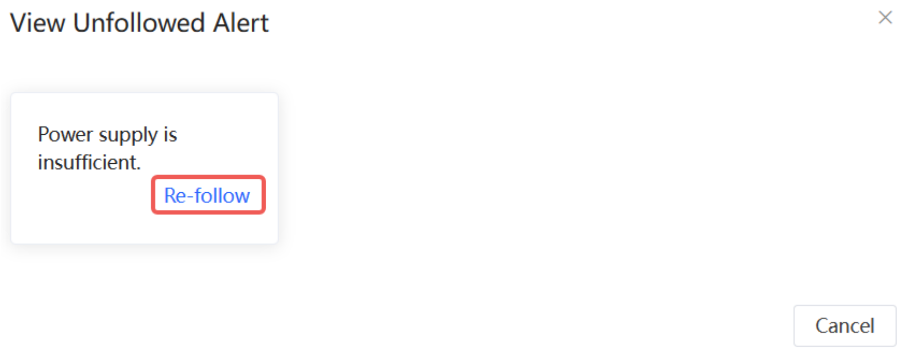
Click **View Unfollowed Alert** to view the unfollowed alert. You can follow the alert again in the pop-up window.



View and manage alarms.

Alert List

Expand	Alerts	Suggestion	Action
No Data			



View Unfollowed Alert

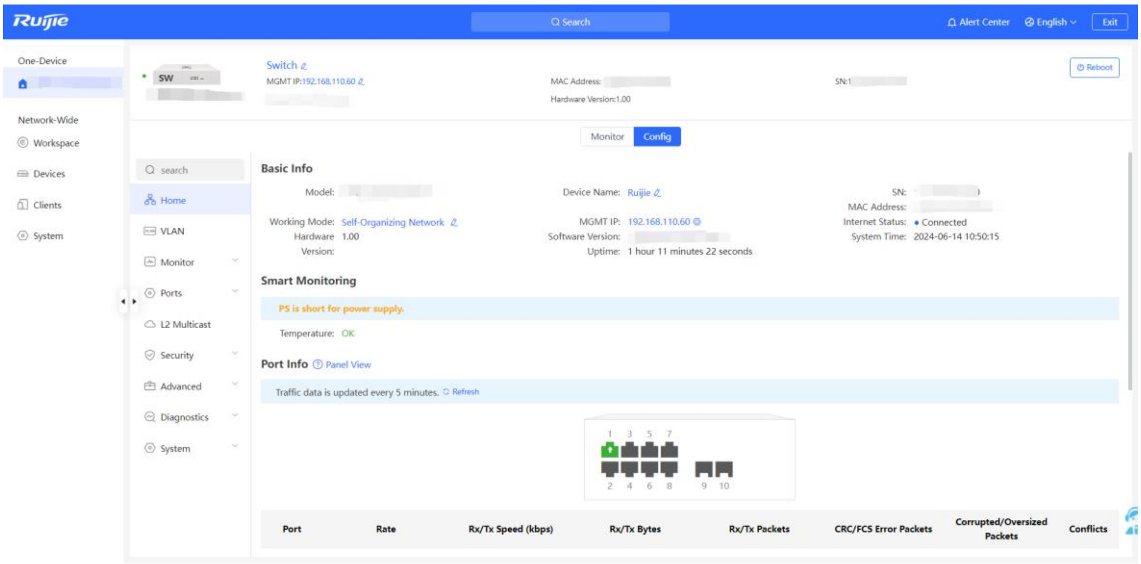
Power supply is insufficient.

4 One-Device Information

4.1 Basic information about the One-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.



Switch
MGMT IP:192.168.110.60
MAC Address: [redacted]
Hardware Version:1.00
SN:[redacted]

Basic Info

Model: [redacted]
Device Name: Ruijie
SN: [redacted]
MAC Address: [redacted]
Working Mode: Self-Organizing Network
MGMT IP: 192.168.110.60
Internet Status: ● Connected
Hardware Version: 1.00
Software Version: [redacted]
System Time: 2024-06-14 10:50:15
Uptime: 1 hour 11 minutes 22 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK

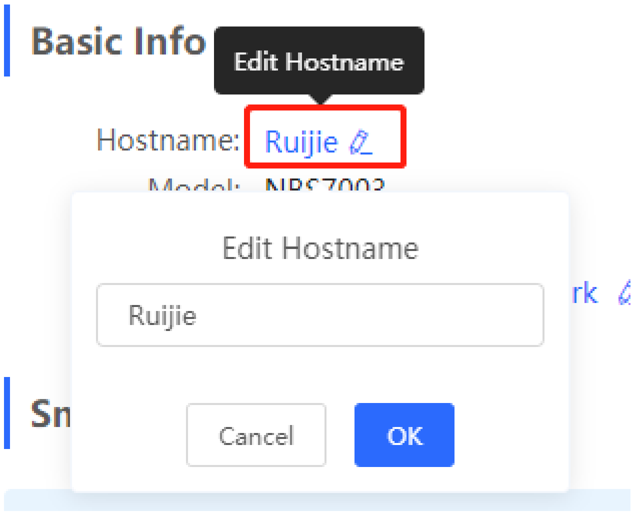
Port Info Panel View

Traffic data is 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

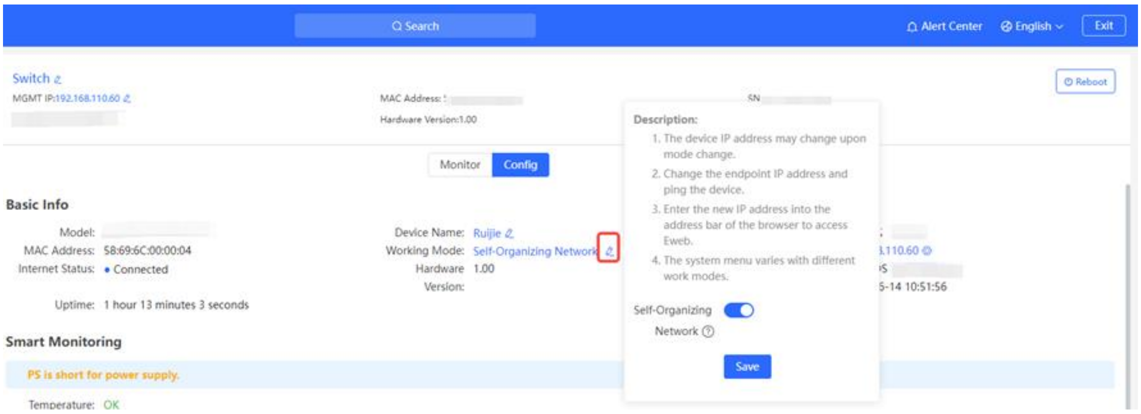
1. Setting the device name

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



2. Switching the Work Mode

Click the current work mode to change the work mode.



MGMT IP:192.168.110.60

MAC Address:

Hardware Version:1.00

SN

Basic Info

Model:

MAC Address: 58:69:6C:00:00:04

Internet Status: ● Connected

Uptime: 1 hour 13 minutes 3 seconds

Device Name: Ruijie

Working Mode: Self-Organizing Network

Hardware Version: 1.00

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

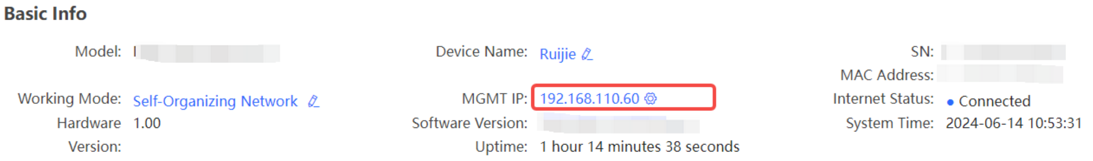
Smart Monitoring

PS is short for power supply.

Temperature: OK

3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see 7.6 MGMT IP Configuration.



Basic Info

Model:

Working Mode: Self-Organizing Network

Hardware Version: 1.00

Device Name: Ruijie

MGMT IP: 192.168.110.60

Software Version:

Uptime: 1 hour 14 minutes 38 seconds

SN:

MAC Address:

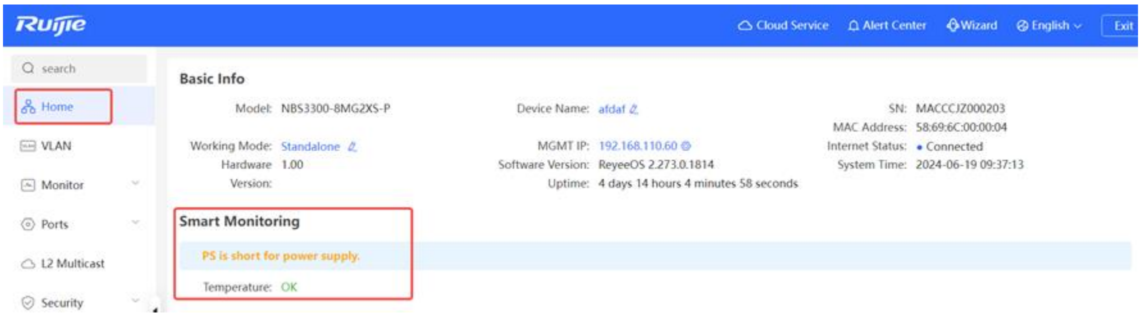
Internet Status: ● Connected

System Time: 2024-06-14 10:53:31

4.2 Smart Monitoring

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

Model: NBS3300-8MG2XS-P

Working Mode: Standalone

Hardware Version: 1.00

Device Name: afdaf

MGMT IP: 192.168.110.60

Software Version: ReyeeOS 2.273.0.1814

Uptime: 4 days 14 hours 4 minutes 58 seconds

SN: MACCCJZ000203

MAC Address: 58:69:6C:00:00:04

Internet Status: ● Connected

System Time: 2024-06-19 09:37:13

Smart Monitoring

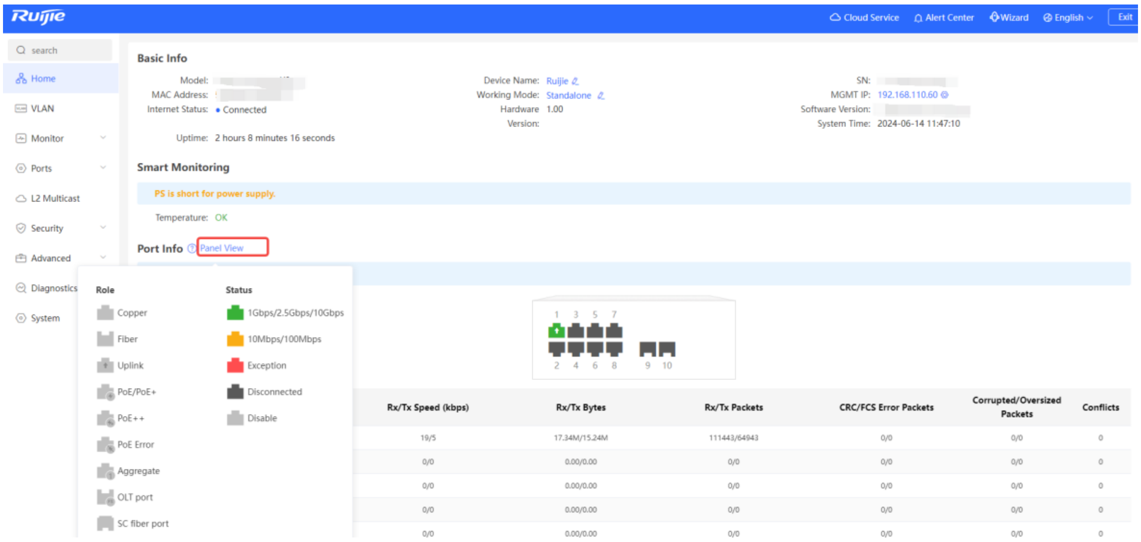
PS is short for power supply.

Temperature: OK

4.3 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.



Basic Info

Model: [redacted]
MAC Address: [redacted]
Internet Status: ● Connected
Uptime: 2 hours 8 minutes 16 seconds
Device Name: Ruijie
Working Mode: Standalone
Hardware Version: 1.00
SN: [redacted]
MGMT IP: 192.168.110.60
Software Version: [redacted]
System Time: 2024-06-14 11:47:10

Smart Monitoring

PS is short for power supply.

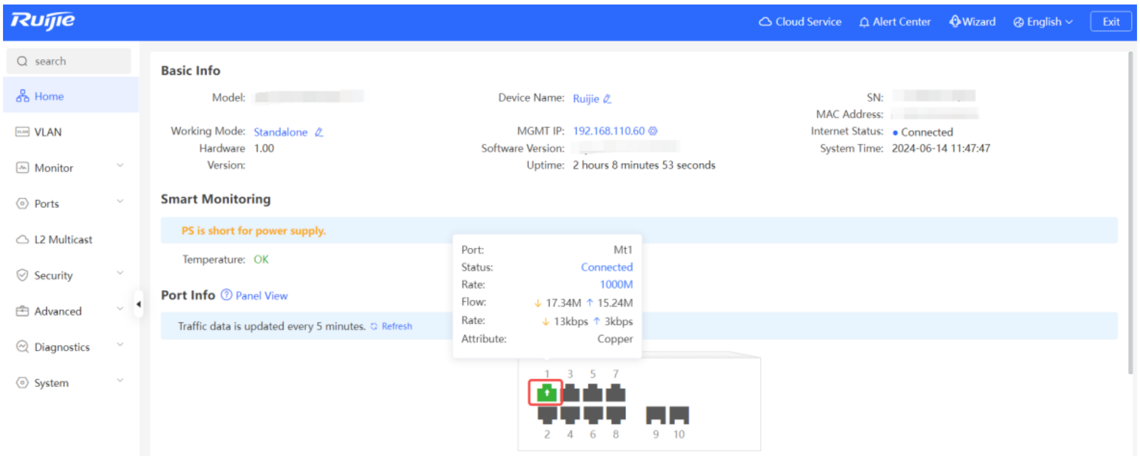
Temperature: OK

Port Info Panel View

Role	Status
Copper	🟩 1Gbps/2.5Gbps/10Gbps
Fiber	🟧 10Mbps/100Mbps
Uplink	🟥 Exception
PoE/PoE+	■ Disconnected
PoE++	□ Disable
PoE Error	
Aggregate	
OLT port	
SC fiber port	

Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
19/5	17.34M/15.24M	111443/64943	0/0	0/0	0
0/0	0.00/0.00	0/0	0/0	0/0	0
0/0	0.00/0.00	0/0	0/0	0/0	0
0/0	0.00/0.00	0/0	0/0	0/0	0
0/0	0.00/0.00	0/0	0/0	0/0	0

- 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.



Basic Info

Model: [redacted]
Working Mode: Standalone
Hardware Version: 1.00
Device Name: Ruijie
MGMT IP: 192.168.110.60
Software Version: [redacted]
Uptime: 2 hours 8 minutes 53 seconds
SN: [redacted]
MAC Address: [redacted]
Internet Status: ● Connected
System Time: 2024-06-14 11:47:47

Smart Monitoring

PS is short for power supply.

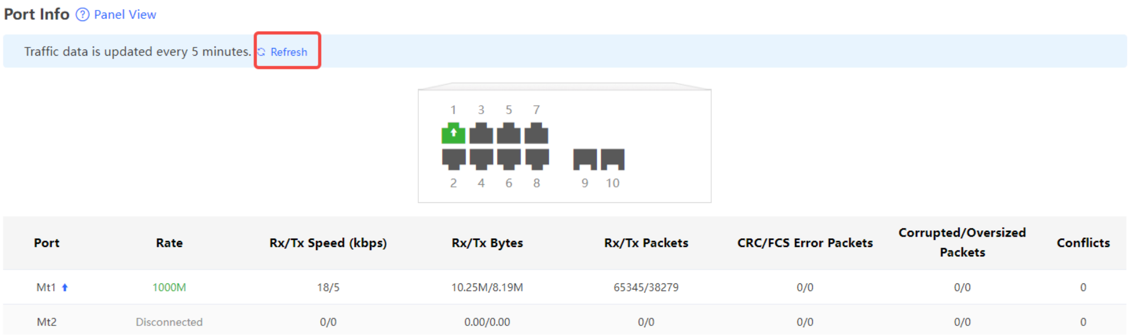
Temperature: OK

Port Info Panel View

Traffic data is updated every 5 minutes. Refresh

Port: Mt1
Status: Connected
Rate: 1000M
Flow: ↓ 17.34M ↑ 15.24M
Rate: ↓ 13kbps ↑ 3kbps
Attribute: Copper

- 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

Traffic data is 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
Mt1 ↑	1000M	18/5	10.25M/8.19M	65345/38279	0/0	0/0	0
Mt2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

5 VLAN

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.

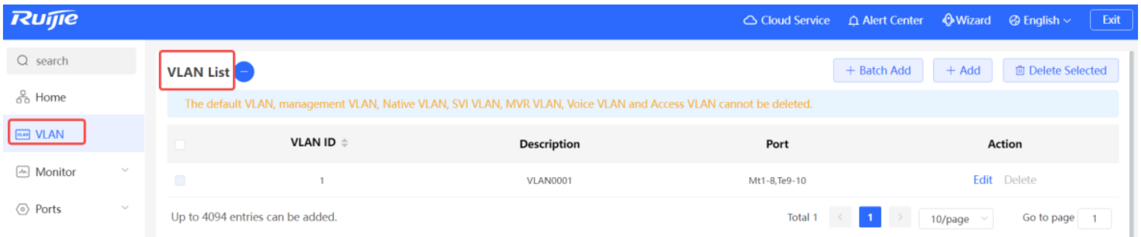
When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs. VLANs can make L3 communication with each other through L3 devices or L3 interfaces.

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

5.2 Configuring 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.



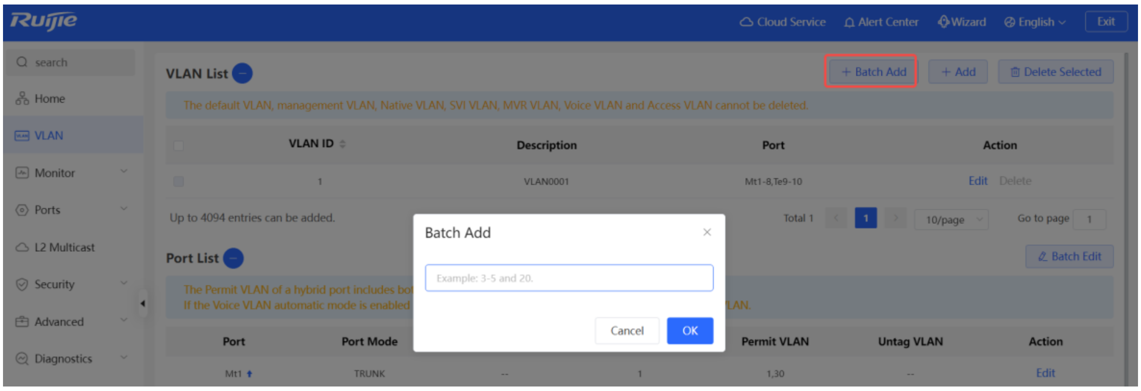
The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.

VLAN ID	Description	Port	Action
1	VLAN0001	Mt1-8,Te9-10	Edit Delete

Up to 4094 entries can be added.

5.2.1 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**.



The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.

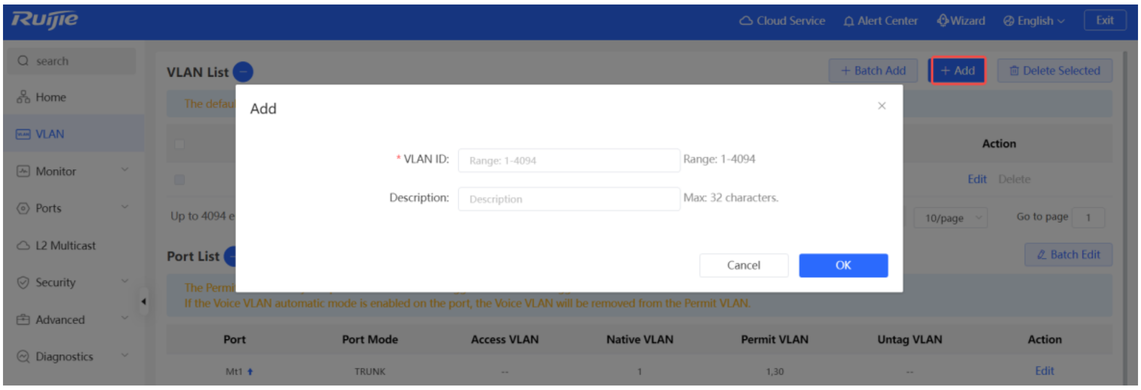
VLAN ID	Description	Port	Action
1	VLAN0001	Mt1-8,Te9-10	Edit Delete

Up to 4094 entries can be added.

The Permit VLAN of a hybrid port includes bo
If the Voice VLAN automatic mode is enabled
LAN.

Port	Port Mode			Permit VLAN	Untag VLAN	Action
Mt1	TRUNK	--	1	1,30	--	Edit

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**.



Add

* VLAN ID: Range: 1-4094 Range: 1-4094

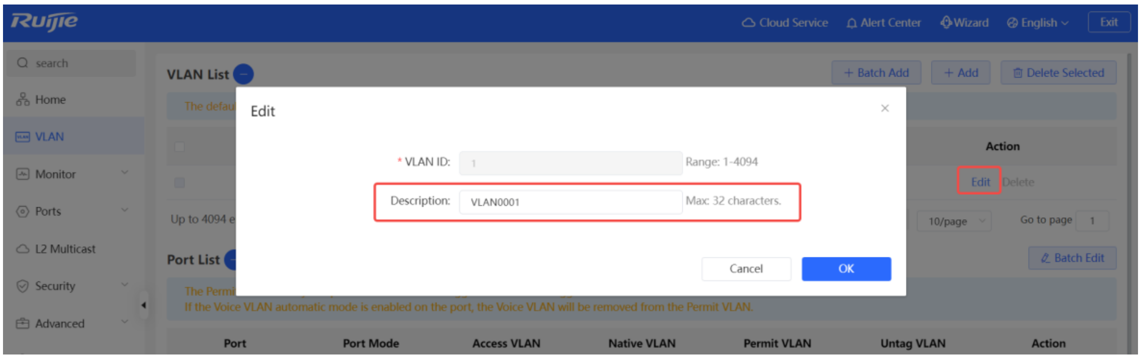
Description: Description Max: 32 characters.

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.

5.2.2 Modifying VLAN Description

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



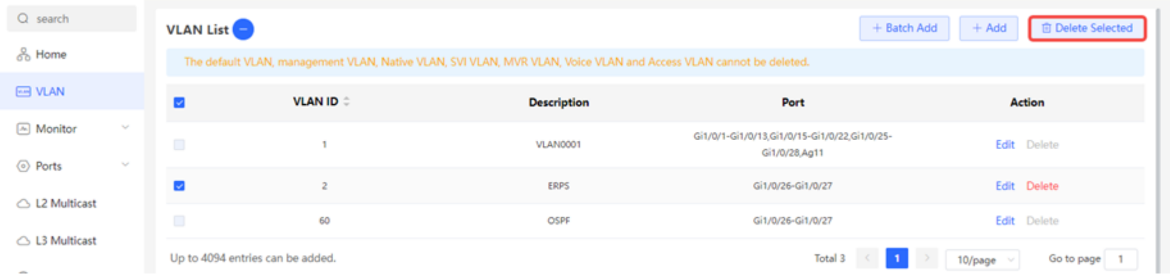
Edit

* VLAN ID: 1 Range: 1-4094

Description: VLAN0001 Max: 32 characters.

5.2.3 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.

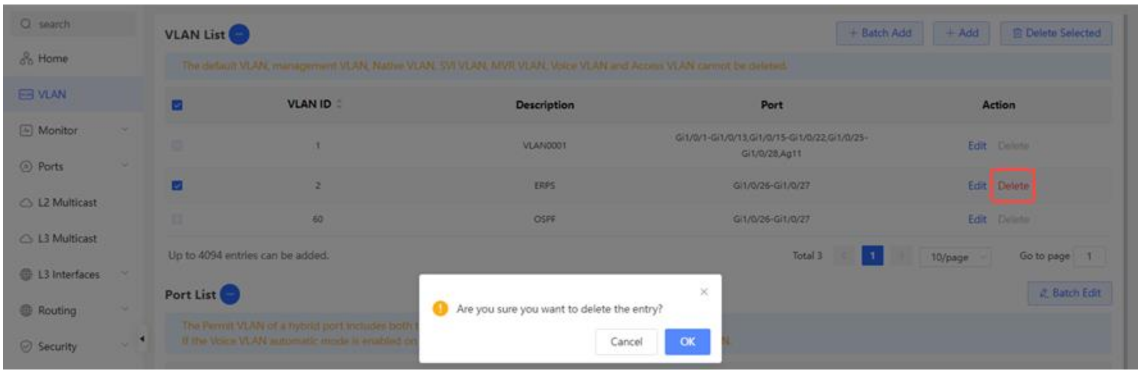


The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.

☑	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi1/0/1-Gi1/0/13,Gi1/0/15-Gi1/0/22,Gi1/0/25-Gi1/0/28,Ag11	Edit Delete
☑	2	ERPS	Gi1/0/26-Gi1/0/27	Edit Delete
□	60	OSPF	Gi1/0/26-Gi1/0/27	Edit Delete

Up to 4094 entries can be added.

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



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	Gi1/0/1-Gi1/0/13,Gi1/0/15-Gi1/0/22,Gi1/0/25-Gi1/0/28,Ag11	Edit Delete
☑	2	ERPS	Gi1/0/26-Gi1/0/27	Edit Delete
□	60	OSPF	Gi1/0/26-Gi1/0/27	Edit Delete

Up to 4094 entries can be added.

The Permit VLAN of a hybrid port includes both t
If the Voice VLAN automatic mode is enabled on

Are you sure you want to delete the entry?

Note

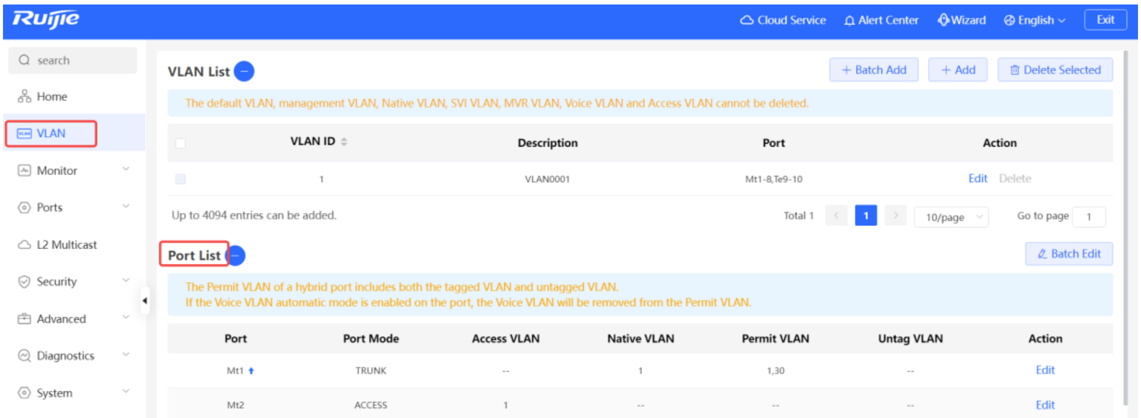
The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. For these VLANs, the **Delete** button is unavailable in gray.

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 3.5.2 Creating a VLAN) and then configure the port based on the VLANs.



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	Mt1-8,Te9-10	Edit Delete

Up to 4094 entries can be added.

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
Mt1 ↑	TRUNK	--	1	1,30	--	Edit
Mt2	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 5-1 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 Untagged VLAN. The frames forwarded by the hybrid port from a Tag VLAN carry tags, and the frames forwarded by the hybrid port from an Untagged VLAN do not carry tags. The frames forwarded by the hybrid port from Native VLAN must not carry tags, therefore Native VLAN can only belong to Untagged VLAN List.

Note

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

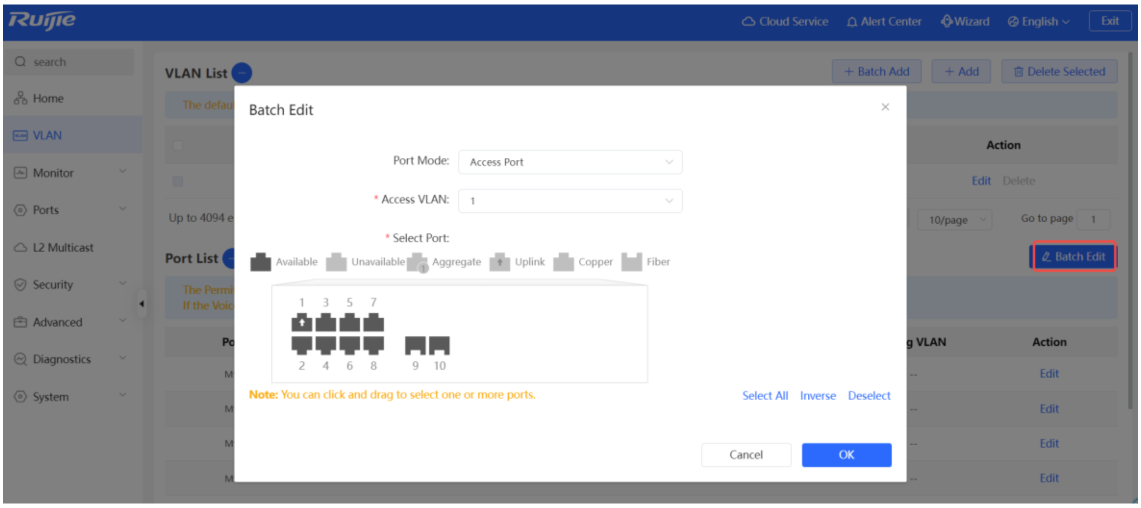
2. Procedure

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 Untagged VLAN range. Click **OK** to complete the batch configuration.

Note

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



Batch Edit

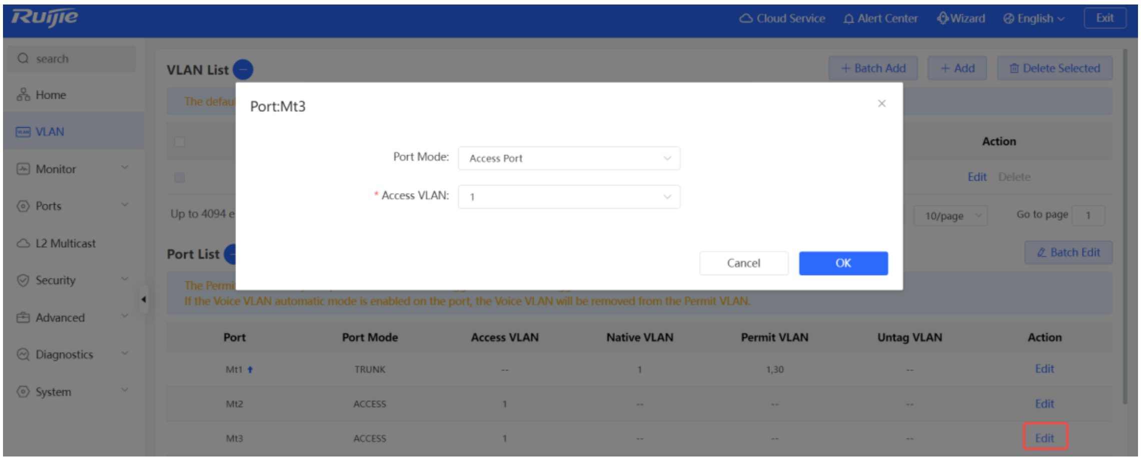
Port Mode: Access Port

* 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 **Action** column of a specified port, configure the port mode and corresponding VLAN, and click **OK**.



Port:Mt3

Port Mode: Access Port

* Access VLAN: 1

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
Mt1	TRUNK	--	1	1,30	--	Edit
Mt2	ACCESS	1	--	--	--	Edit
Mt3	ACCESS	1	--	--	--	Edit

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 web interface. Therefore, exercise caution when configuring VLANs.

5.4 Batch Switch Configuration

1. Overview

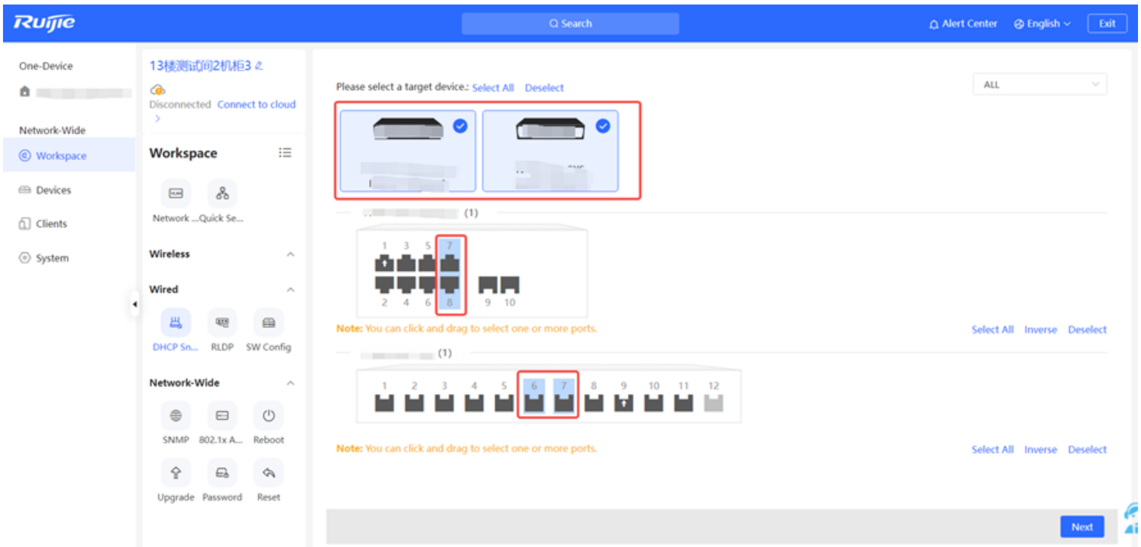
You can batch create VLANs, configure port attributes, and divide port VLANs for switches on the network.

2. Procedure

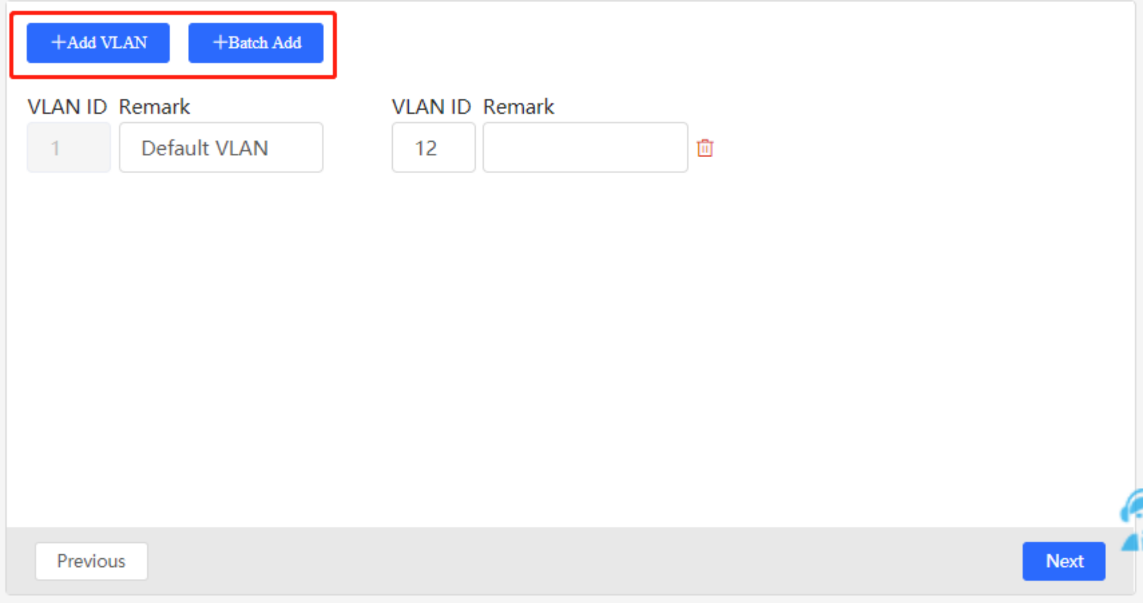
Choose **Network-Wide > Workspace** > **Wired** > **SW Config**.

(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

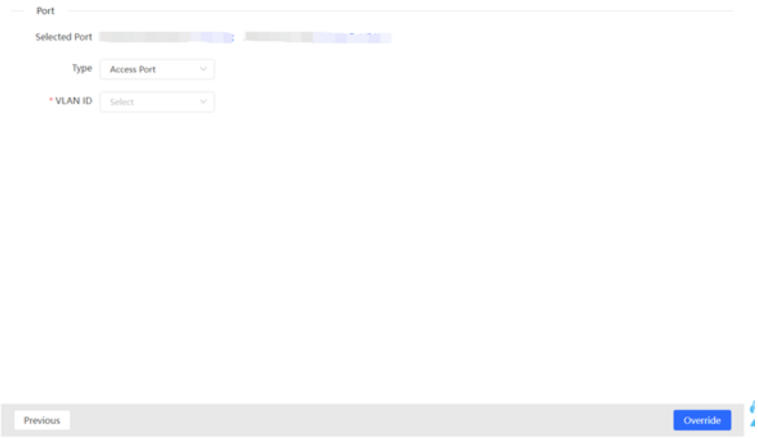
network, select a product model from the drop-down list box to filter the devices. After the desired devices and ports are selected, click **Next**.



(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**.



(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.



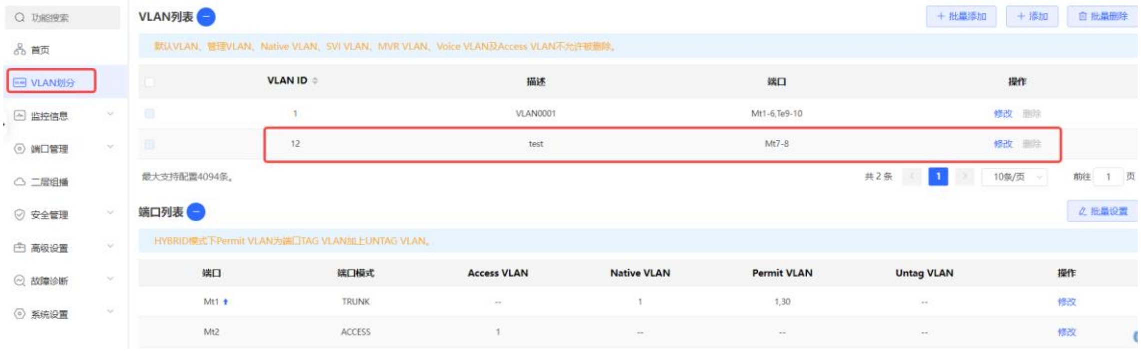
Selected Port

Type: Access Port

* VLAN ID: Select

3. Verifying Configuration

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



VLAN列表

默认VLAN、管理VLAN、Native VLAN、SVI VLAN、MVR VLAN、Voice VLAN及Access VLAN不允许被删除。

□	VLAN ID	描述	端口	操作
□	1	VLAN0001	Mt1-6,Te9-10	修改 删除
□	12	test	Mt7-8	修改 删除

最大支持配置4094条。 共 2 条 1 10条/页 前往 1 页

端口列表

HYBRID模式下Permit VLAN为端口TAG VLAN加上UNTAG VLAN。

端口	端口模式	Access VLAN	Native VLAN	Permit VLAN	Untag VLAN	操作
Mt1 ↑	TRUNK	--	1	1,30	--	修改
Mt2	ACCESS	1	--	--	--	修改

6 Monitoring

6.1 Port Flow

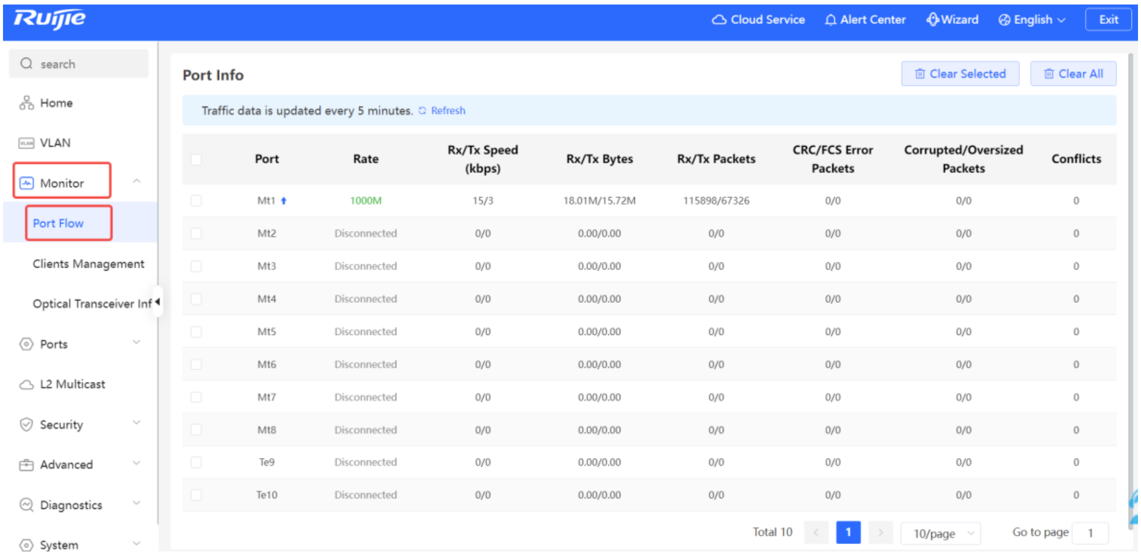
Choose **Local Device** > **Monitor** > **Port Flow**.

This page displays 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 interfaces can be configured. Traffic of an aggregate interface is the sum of traffic of all member ports.



Port Info

Clear Selected Clear All

Traffic data is 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
□	Mt1 ↑	1000M	15/3	18.01M/15.72M	115898/67326	0/0	0/0	0
□	Mt2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt3	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt7	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Mt8	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Te9	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Te10	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

Total 10 < 1 > 10/page Go to page 1

6.2 Client Management

6.2.1 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

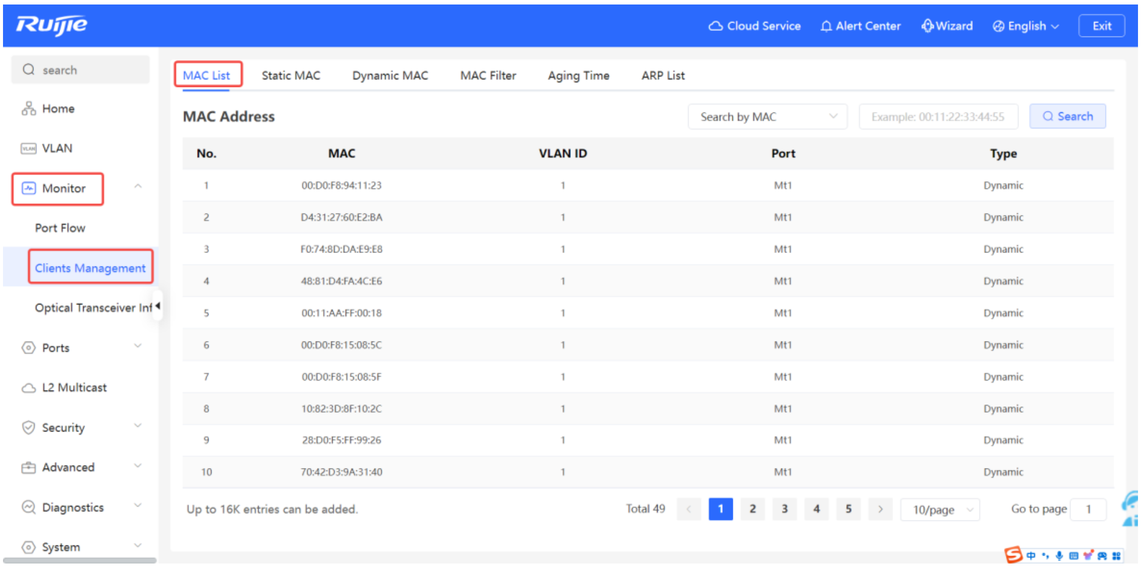
This section describes the management of static, dynamic, and filtering MAC address entries, and does not cover multicast MAC address entries.

6.2.2 Displaying the MAC Address Table

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

This page 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: Query 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. Fuzzy search is supported.



MAC Address

No.	MAC	VLAN ID	Port	Type
1	00:D0:F8:94:11:23	1	Mt1	Dynamic
2	D4:31:27:60:E2:BA	1	Mt1	Dynamic
3	F0:74:8D:DA:E9:E8	1	Mt1	Dynamic
4	48:81:D4:FA:4C:E6	1	Mt1	Dynamic
5	00:11:AA:FF:00:18	1	Mt1	Dynamic
6	00:D0:F8:15:08:5C	1	Mt1	Dynamic
7	00:D0:F8:15:08:5F	1	Mt1	Dynamic
8	10:82:3D:8F:10:2C	1	Mt1	Dynamic
9	28:D0:F5:FF:99:26	1	Mt1	Dynamic
10	70:42:D3:9A:31:40	1	Mt1	Dynamic

Up to 16K entries can be added.

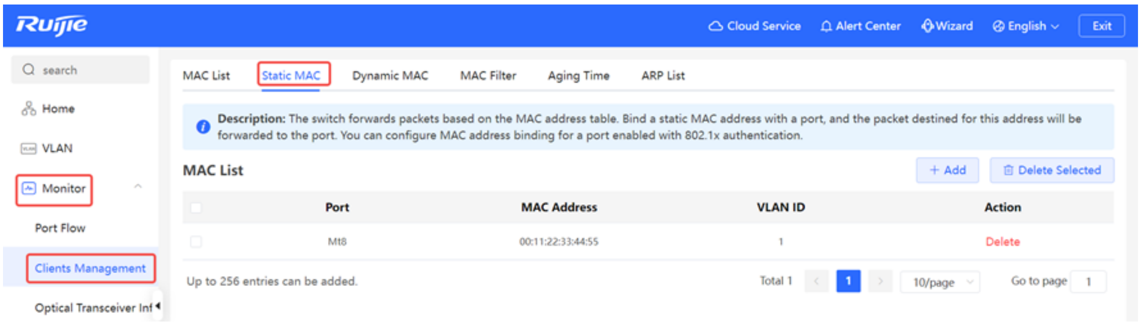
Total 49 1 2 3 4 5 10/page Go to page 1

Note

The MAC address entry capacity depends on the product. For example, the MAC address entry capacity of the device shown in the preceding figure is 32000.

6.2.3 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 to 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.



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

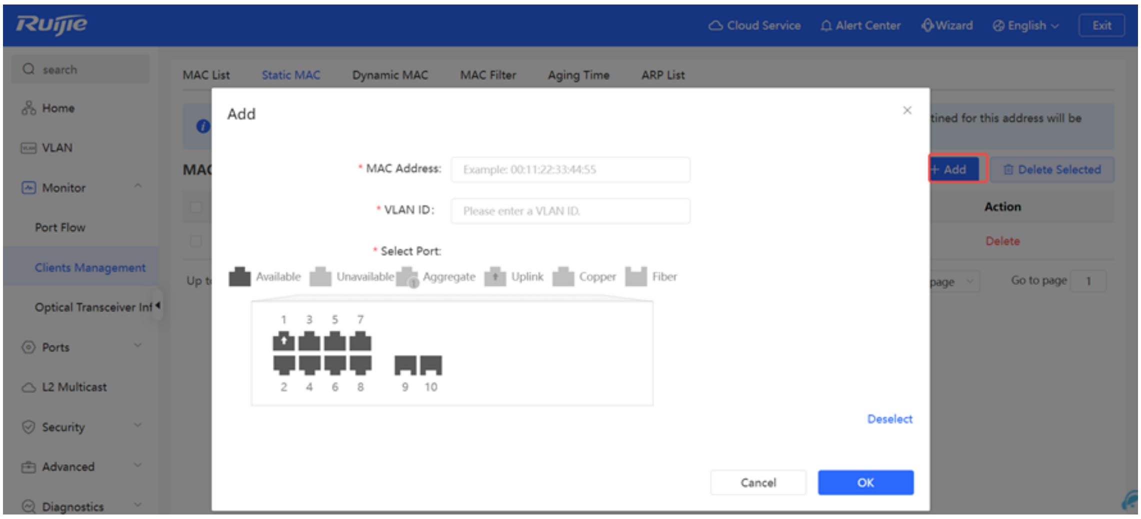
Port	MAC Address	VLAN ID	Action
Mt8	00:11:22:33:44:55	1	Delete

Up to 256 entries can be added.

1. Adding Static MAC Address Entries

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

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



Add

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

* VLAN ID: Please enter a VLAN ID.

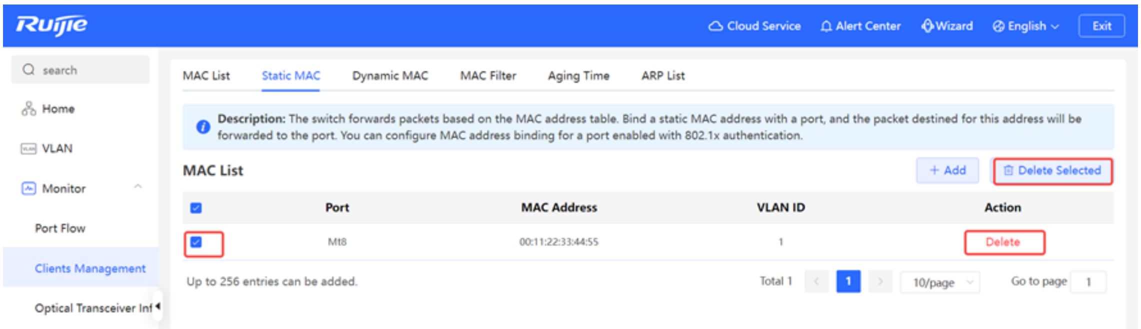
* Select Port:

2. Deleting Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients Management** > **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**, select the entry to be deleted, click **Delete** in the **Action** column. In the displayed dialog box, click **OK**.



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

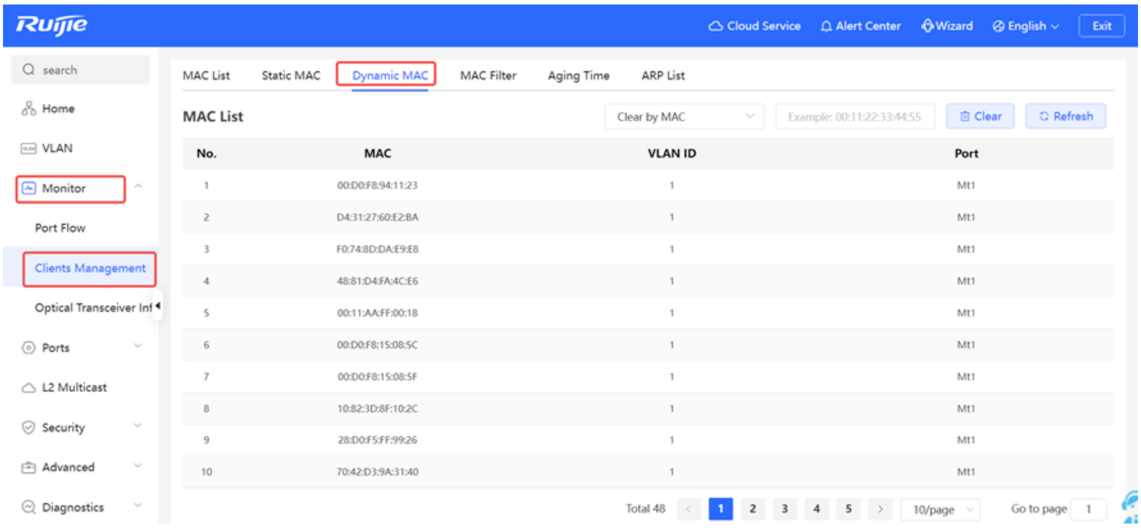
☑	Port	MAC Address	VLAN ID	Action
☑	Mt8	00:11:22:33:44:55	1	Delete

Up to 256 entries can be added.

6.2.4 Displaying Dynamic MAC Address

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

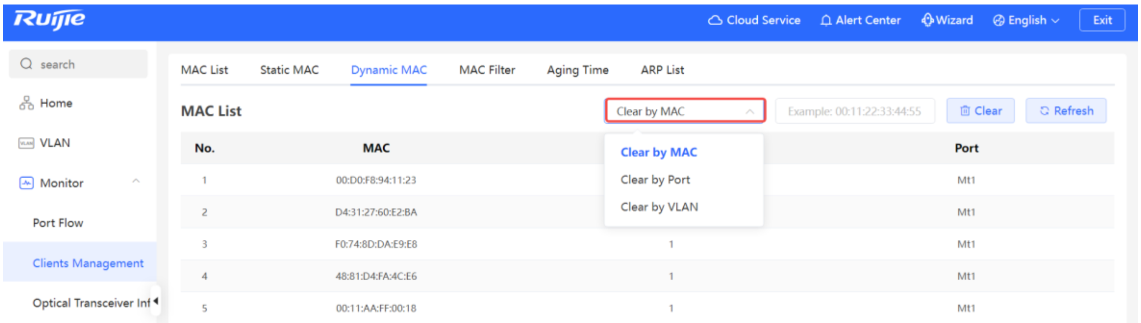
After receiving a packet, the device will automatically generate dynamic MAC address entries based on the source MAC address of the packet. The current page displays the dynamic MAC address entries learned by the device. Click **Refresh** to obtain the latest dynamic MAC address entries.



MAC List

No.	MAC	VLAN ID	Port
1	00:D0:F8:94:11:23	1	Mt1
2	D4:31:27:60:E2:BA	1	Mt1
3	F0:74:8D:DA:E9:E8	1	Mt1
4	48:81:D4:FA:4C:E6	1	Mt1
5	00:11:AA:FF:00:18	1	Mt1
6	00:D0:F8:15:08:5C	1	Mt1
7	00:D0:F8:15:08:5F	1	Mt1
8	10:82:3D:8F:10:2C	1	Mt1
9	28:D0:F5:FF:99:26	1	Mt1
10	70:42:D3:9A:31:40	1	Mt1

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.

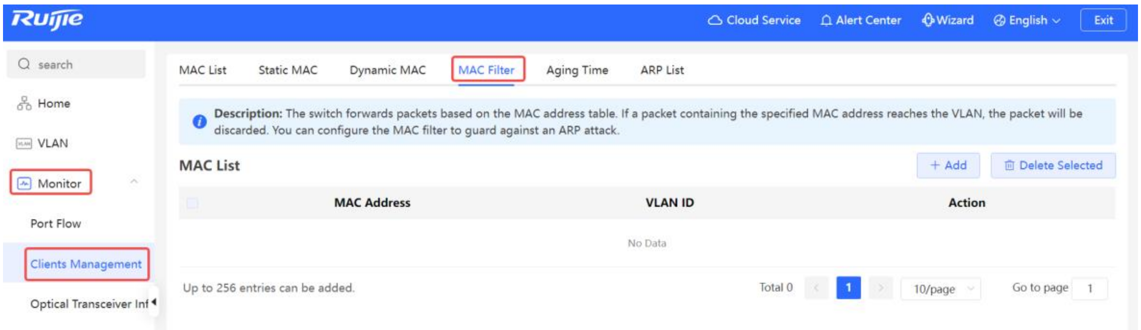


MAC List

No.	MAC		Port
1	00:D0:F8:94:11:23		Mt1
2	D4:31:27:60:E2:BA		Mt1
3	F0:74:8D:DA:E9:E8	1	Mt1
4	48:81:D4:FA:4C:E6	1	Mt1
5	00:11:AA:FF:00:18	1	Mt1

6.2.5 Configuring MAC Address Filtering

To prohibit a user from sending and receiving packets in certain scenarios, you can add MAC addresses 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.



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.

MAC List　+ Add　Delete Selected

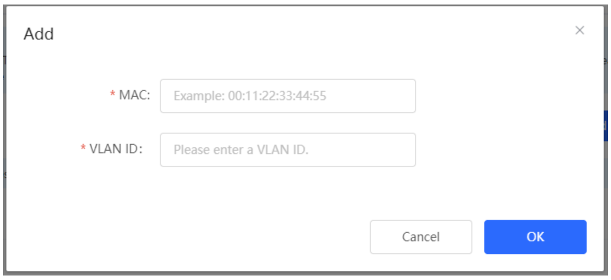
□	MAC Address	VLAN ID	Action
No Data			

Up to 256 entries can be added.　Total 0　1　10/page　Go to page 1

1. Adding Filtering MAC Address

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

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



Add

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

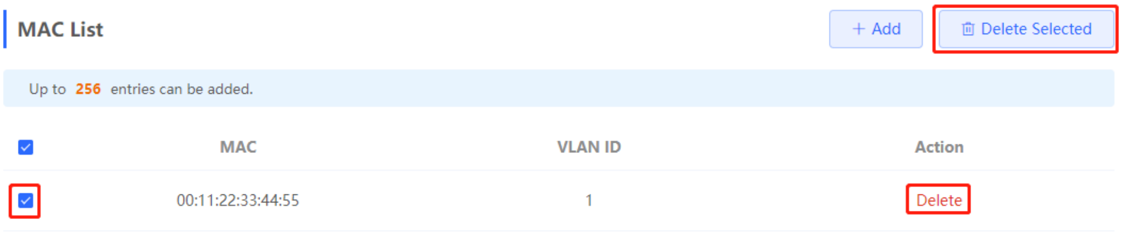
* VLAN ID: Please enter a VLAN ID.

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 **Action** column. In the displayed dialog box, click **OK**.



MAC List　+ Add　Delete Selected

Up to 256 entries can be added.

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

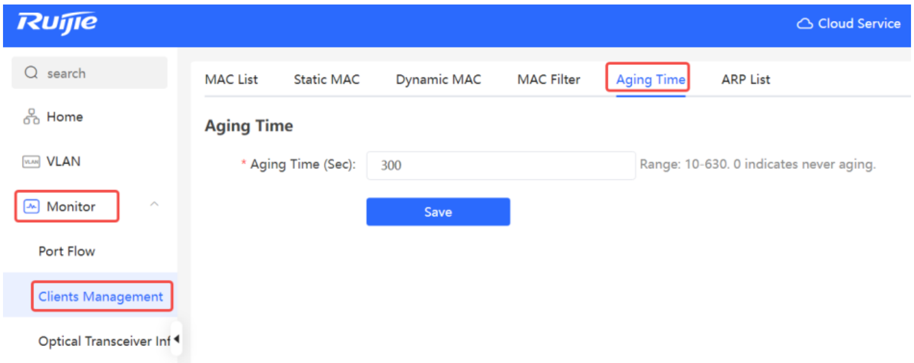
6.2.6 Configuring MAC Address Aging Time

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 indicates no aging.



Aging Time

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

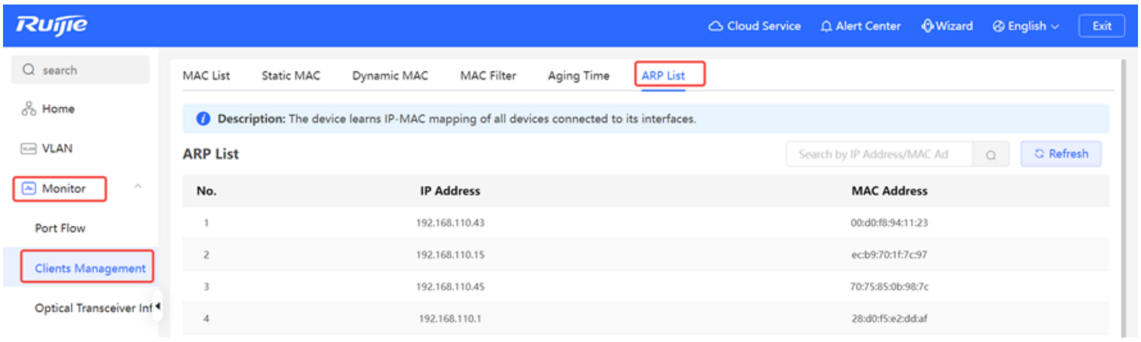
6.2.7 Displaying ARP Information

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. The 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 an IP or MAC address. Click **Refresh** to obtain the latest ARP entries.



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

ARP List

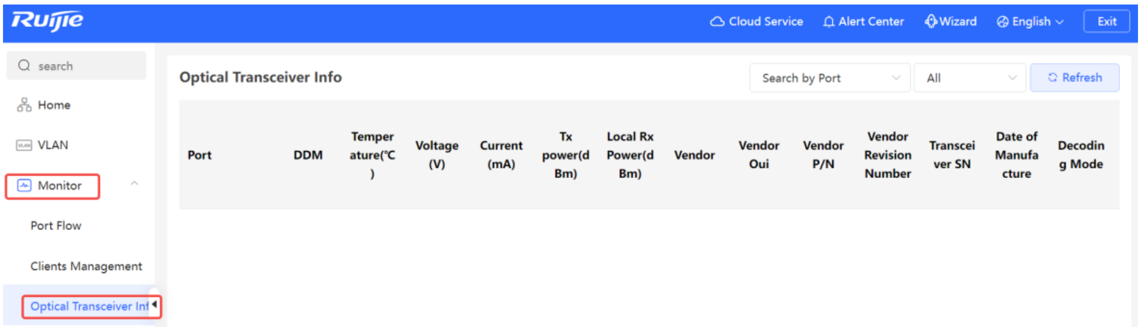
No.	IP Address	MAC Address
1	192.168.110.43	00:d0:f8:94:11:23
2	192.168.110.15	ec:b9:70:1f:7c:97
3	192.168.110.45	70:75:85:0b:98:7c
4	192.168.110.1	28:d0:f5:e2:dd:af

6.3 Viewing Optical Transceiver Info

Choose **Local Device** > **Monitoring** > **Optical Transceiver Info**.

The **Optical Transceiver Info** page displays the basic information of an optical transceiver, including the port to which it is connected, DDM, temperature, voltage, current, transmit power, local receive power, and so on. You can query the information of an optical transceiver by entering the port to which it is connected in the search box.

The data on this page is automatically updated every 5 seconds. You can also click **Refresh** to refresh the optical transceiver information.



Optical Transceiver Info

Port	DDM	Temperature(℃)	Voltage (V)	Current (mA)	Tx power(dBm)	Local Rx Power(dBm)	Vendor	Vendor Oui	Vendor P/N	Vendor Revision Number	Transceiver SN	Date of Manufacture	Decoding Mode

7 Ports

7.1 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 7-1 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

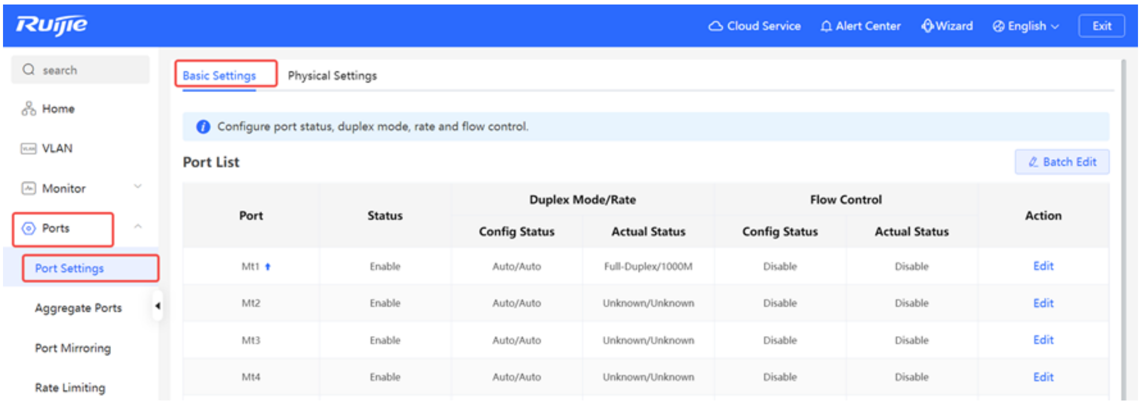
7.2 Port Configuration

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.

7.2.1 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.

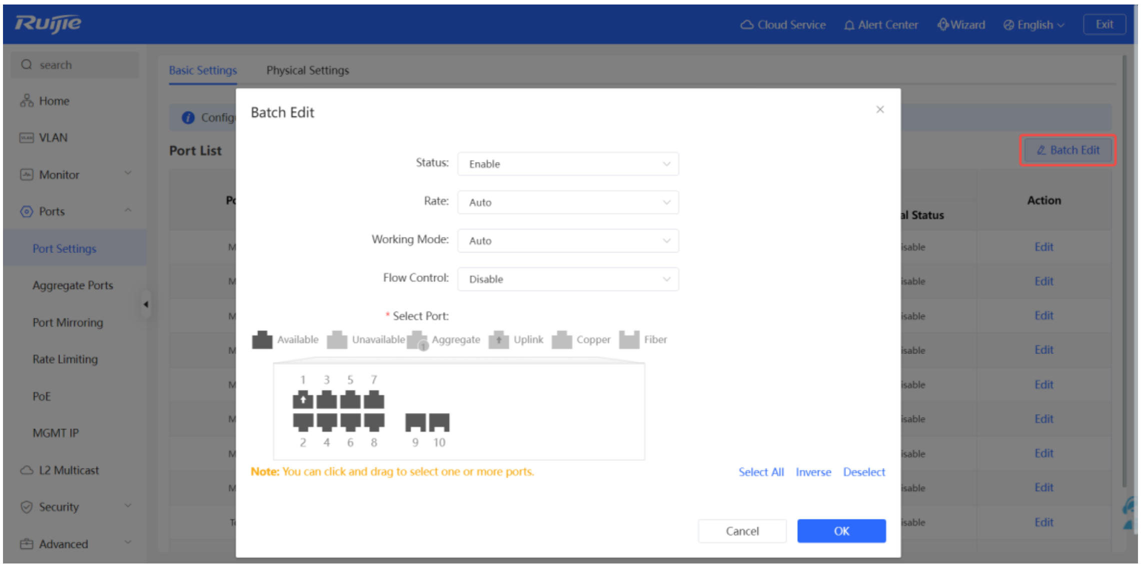


Configure port status, duplex mode, rate and flow control.

Port List

Port	Status	Duplex Mode/Rate		Flow Control		Action
		Config Status	Actual Status	Config Status	Actual Status	
Mt1	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
Mt2	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Mt3	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Mt4	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

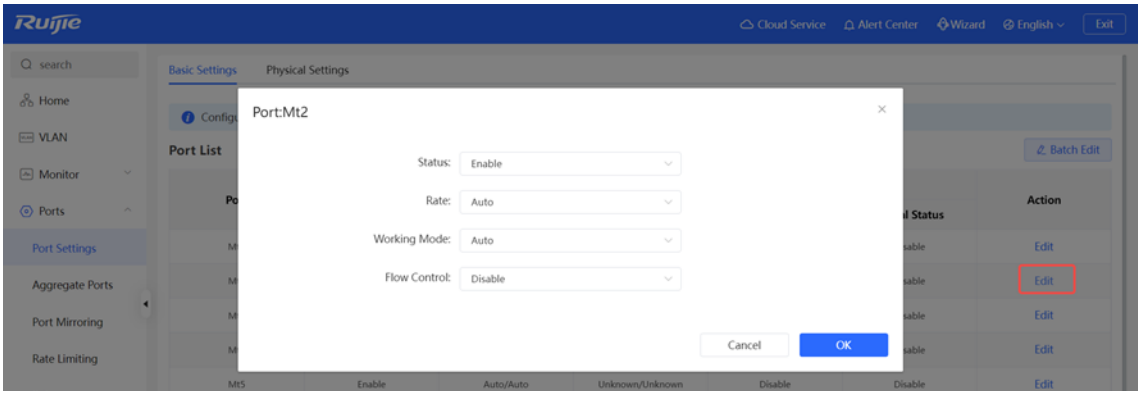
Working Mode: Auto

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**.



Port:Mt2

Status: Enable

Rate: Auto

Working Mode: Auto

Flow Control: Disable

Figure 7-1 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 affected.	Enable
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

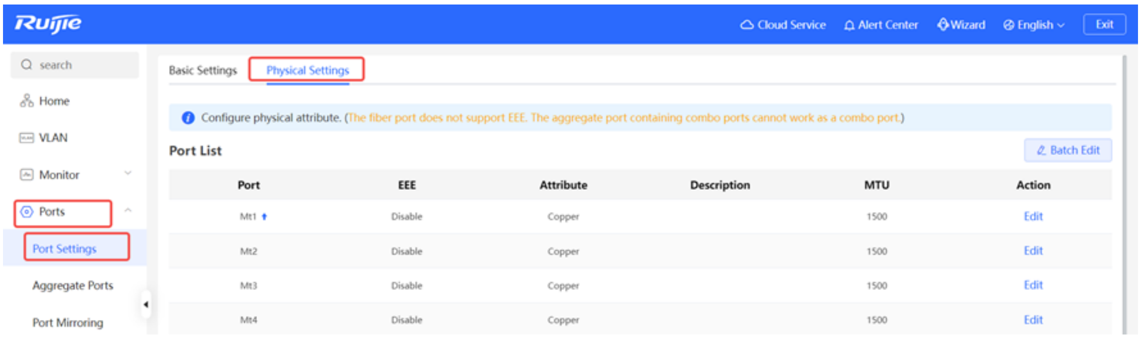
Note

The rate of a 2.5GE port can be set to 2500M, 1000M, 100M, 10M or auto. The rate of a 10G port can be set to 10G, 1000M, or auto.

7.2.2 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.



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

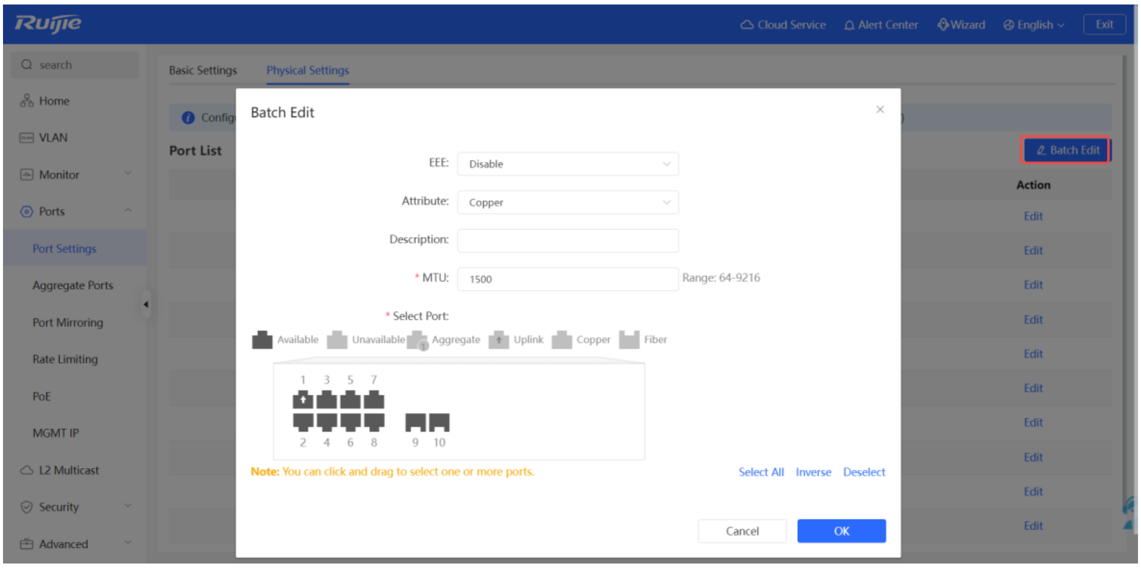
Port List

Port	EEE	Attribute	Description	MTU	Action
Mt1	Disable	Copper		1500	Edit
Mt2	Disable	Copper		1500	Edit
Mt3	Disable	Copper		1500	Edit
Mt4	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

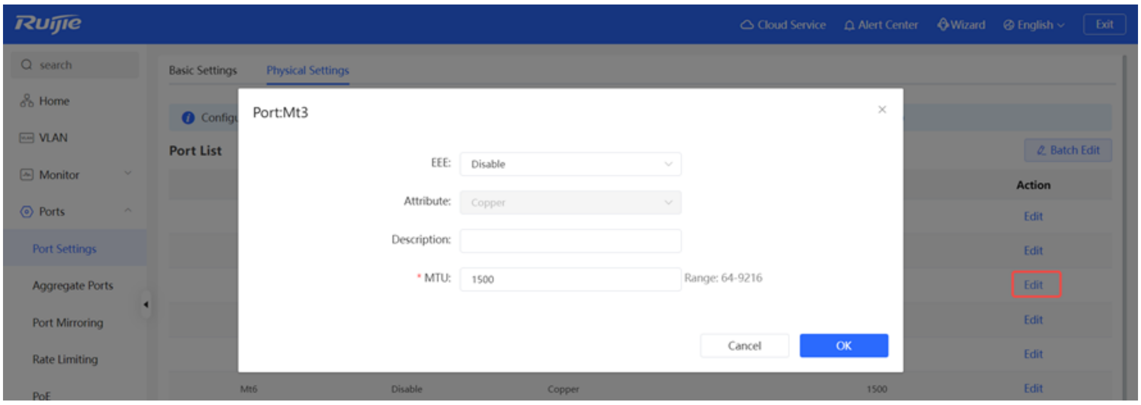
Description:

* 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:Mt3

EEE: Disable

Attribute: Copper

Description:

* MTU: 1500 Range: 64-9216

Table 7-2 **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.
	Copper port: copper mode (cannot be changed);
	SFP port: fiber mode (cannot be changed);
	Only combo ports support mode change.
		Depending on the port attribute

Parameter	Description	Default Value
Description	You can add a description to label the functions of a port.	N/A
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.

7.3 Aggregate Ports

7.3.1 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 x *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.

7.3.2 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. Automatic Aggregation

Automatic 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 automatic 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 an automatic aggregate port, and the corresponding two ports are the member ports of the aggregate port.

Note

- Automatic 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.
- The peer device for automatic aggregation must be RG-EG310G-E.

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

4. LACP

Link Aggregation Control Protocol (LACP) is a standardized protocol for dynamically aggregating multiple physical links into a single logical link to enhance network bandwidth and reliability. LACP defines the negotiation process and parameters of link aggregation, which enables the exchange of link aggregation information and the negotiation of link aggregation parameters among network devices and ensures the reliability and stability of the link aggregation. LACP supports dynamic addition and deletion of links, achieving dynamic link adjustment and optimization.

In LACP, two roles are defined: the actor and the partner. The actor sends a link aggregation request, while the partner responds to the request and joins the link aggregation group.

7.3.3 Aggregate Port Configuration

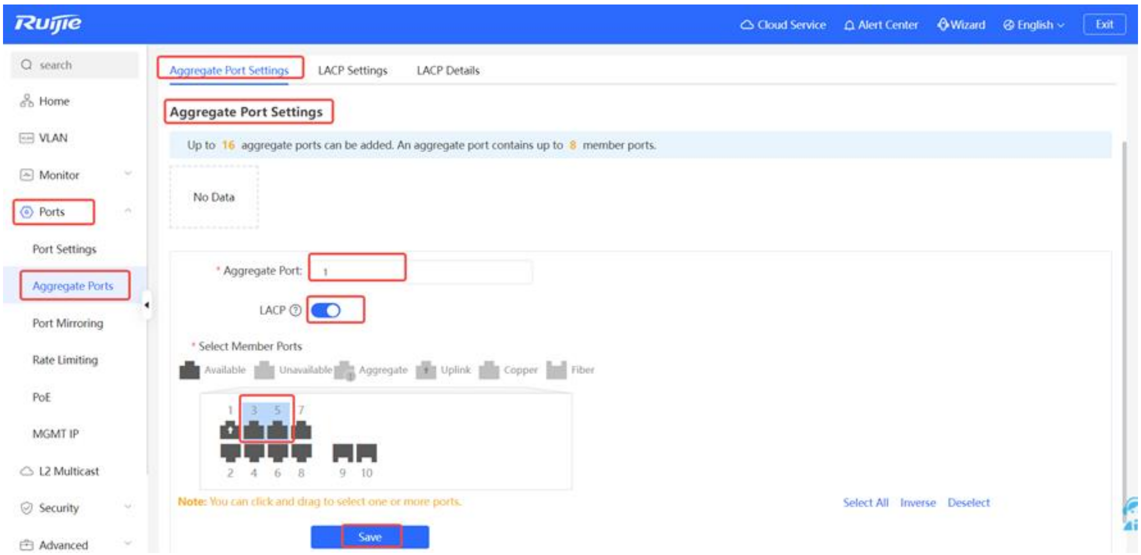
Choose **Local Device** > **Ports** > **Aggregate Ports** > **Aggregate Port Settings**.

1. Adding an Aggregate Port

Enter an aggregate port ID, select member ports (ports that are already a member of an aggregate port cannot be selected), toggle on **LACP**, and click **Save**. You can enable **LACP** to dynamically aggregate links to enhance network reliability and flexibility. 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.
- The LACP state cannot be modified once a static aggregate port is created.



Aggregate Port Settings

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

No Data

* Aggregate Port: 1

LACP ⓘ ●

* Select Member Ports

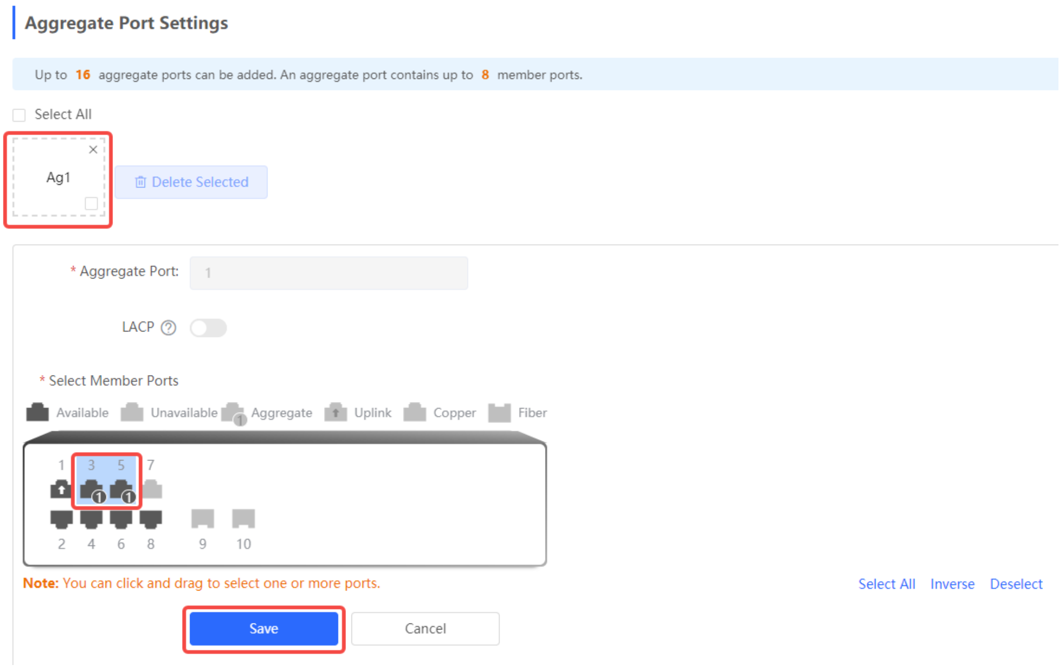
Note: You can click and drag to select one or more ports.

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

Ag1 ×
□

Delete Selected

* Aggregate Port: 1

LACP

* Select Member Ports

Available Unavailable Aggregate Uplink Copper Fiber

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

Select All Inverse Deselect

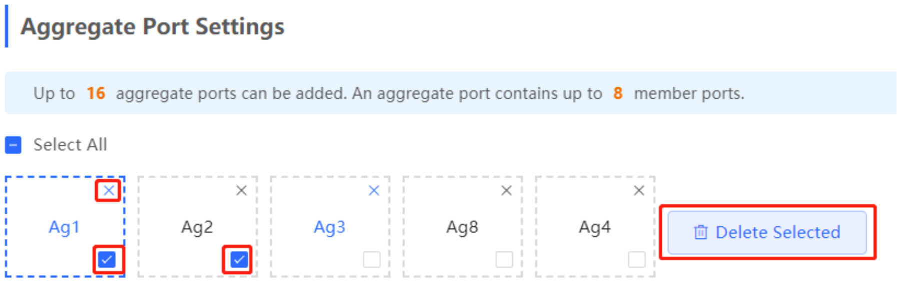
Save Cancel

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

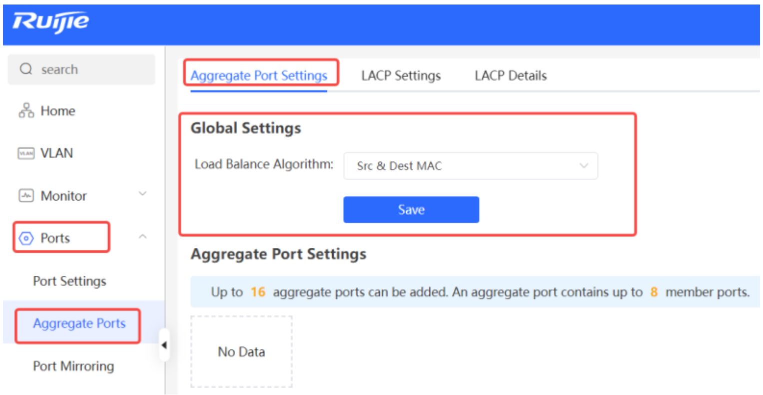
| Ag1 × ☑ | Ag2 × ☑ | Ag3 × □ | Ag8 × □ | Ag4 × □ |

Delete Selected

7.3.4 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

Aggregate Port Settings

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

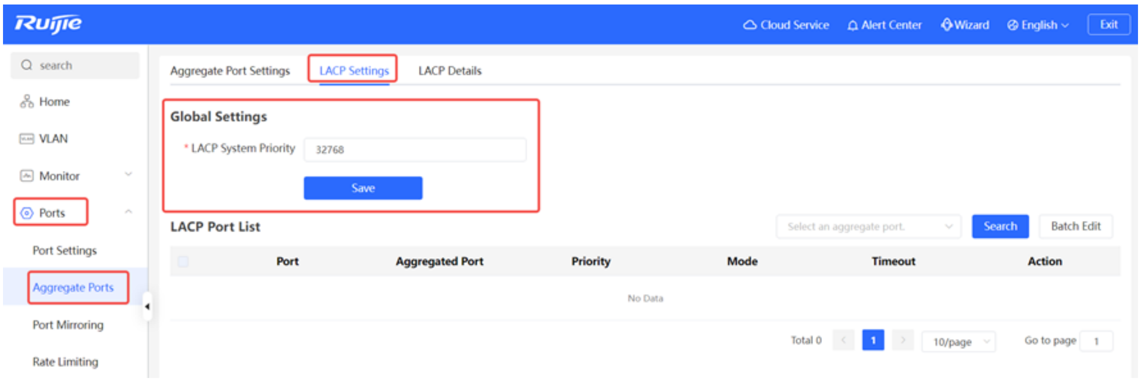
No Data

7.3.5 Configuring LACP Settings

1. LACP System Priority

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

In LACP, the device with a higher system priority becomes the actor in the link aggregation group and controls the working state and parameters of the link aggregation group. The value of system priority ranges from 1 to 65535, and the default value is 32768. The lower the value of system priority, the higher the device priority. When two devices have the same system priority, their MAC addresses are compared, and the device with the smaller MAC address becomes the actor in the link aggregation group.



Global Settings

* LACP System Priority 32768

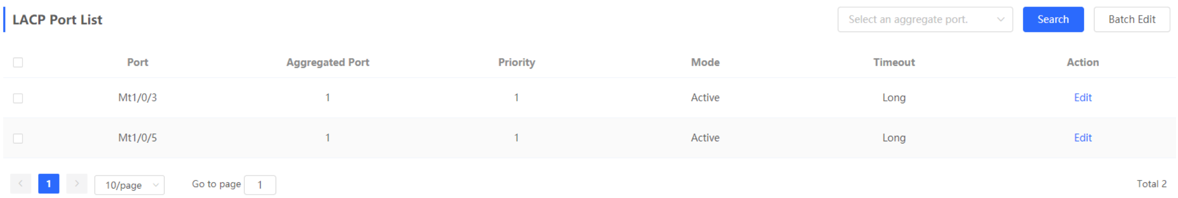
LACP Port List

□	Port	Aggregated Port	Priority	Mode	Timeout	Action
No Data						

Total 0

2. LACP Port List

Choose **Local Device** > **Ports** > **Aggregate Port** > **LACP Settings > LACP Port List**. The **LACP Port List** page shows the port ID, priority, mode, and timeout mode of each LACP-enabled port. You can view the member port details of the corresponding link aggregation group by selecting an aggregate port.

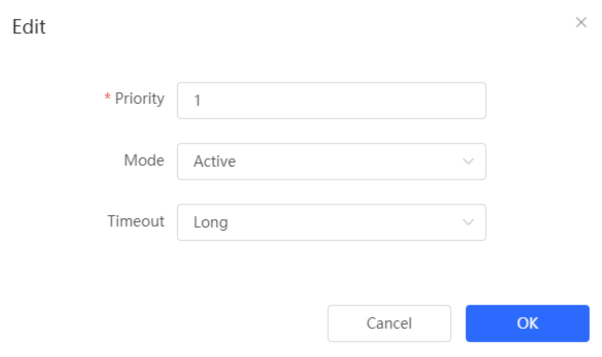


LACP Port List

□	Port	Aggregated Port	Priority	Mode	Timeout	Action
□	Mt1/0/3	1	1	Active	Long	Edit
□	Mt1/0/5	1	1	Active	Long	Edit

Total 2

You can select a specific port and click **Edit**, or select multiple ports and click **Batch Edit** to modify the port priority, mode, and timeout mode in the pop-up window. Then, click **OK** to confirm and apply the changes.



Edit

* Priority: 1

Mode: Active

Timeout: Long

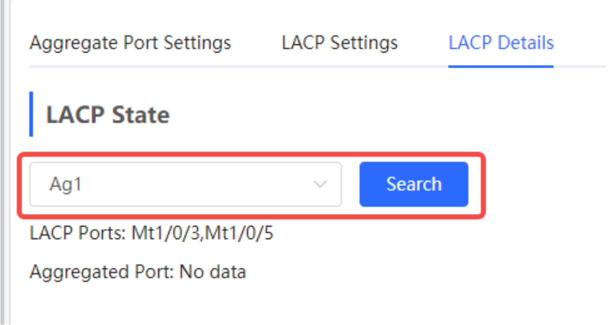
Table 7-3 **Description of LACP Port List Configuration Parameters**

Parameter	**Description**	**Default Value**
Priority	Priority is used to determine which port is the master, with the highest-priority port being selected as the active port. The priority value ranges from 1 to 65535, and a lower priority value indicates a higher priority. If multiple ports have the same priority, their priority ranking is determined by evaluating their port IDs, and the port with the lower port ID will be given a higher priority.	32768
Mode	Mode refers to the method by which two devices within a link aggregation group negotiate their operating mode. ● Active: In active mode, the device assumes the role of the actor and sends requests to establish link aggregation. ● Passive: In passive mode, the device assumes the role of the partner and waits for the peer device to send a request.	Active
Timeout	The purpose of the timeout mode is to determine the timeout period and mechanism for LACP link aggregation. When no LACP frames are received from the peer device within the specified timeout duration, it is assumed that the peer device has experienced a failure. As a result, the failure detection and recovery mechanism of the link aggregation is triggered. ● Long: In long timeout mode, LACP frames are sent every 30 seconds, and the timeout duration is set to 90 seconds. This mode enhances the reliability and stability of link aggregation, but it can potentially lead to delayed detection of faults. ● Short: In short timeout mode, LACP frames are sent every second, and the timeout duration is set to 3 seconds. This mode enhances the response speed of link aggregation and ensures timely fault detection, but it may impose additional network load and resource consumption.	Long

3. Viewing LACP State

Choose **Local Device** > **Ports** > **Aggregate Port** > **LACP Details**.

You can select an LACP-enabled aggregate port and click **Search** to view the LACP-enabled member ports and the aggregate port information on this page.



LACP Ports: Mt1/0/3,Mt1/0/5

Aggregated Port: No data

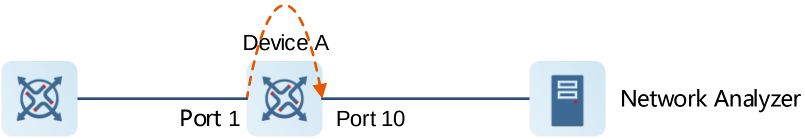
7.4 Port Mirroring

7.4.1 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 7-2 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.

7.4.2 Procedure

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

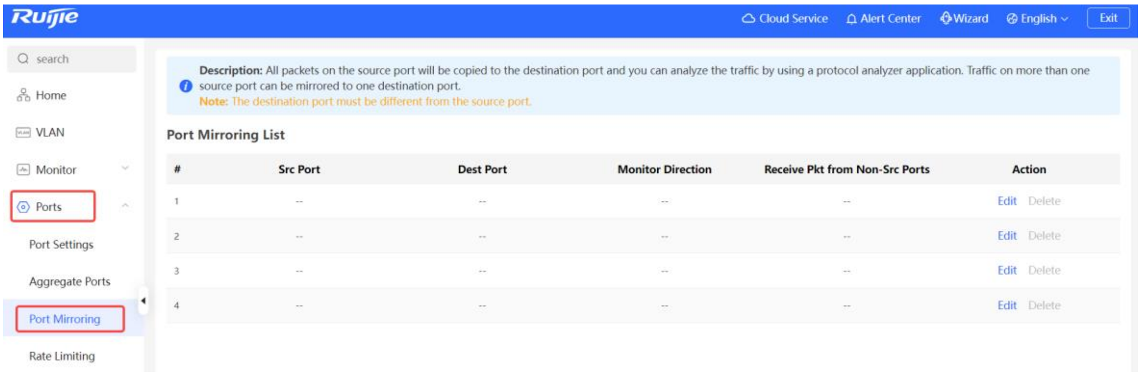
Click **Edit**, select the source port, destination port, monitor direction, and whether to receive packets from non-source ports, and click **OK**. A maximum of four SPAN entries can be configured.

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.

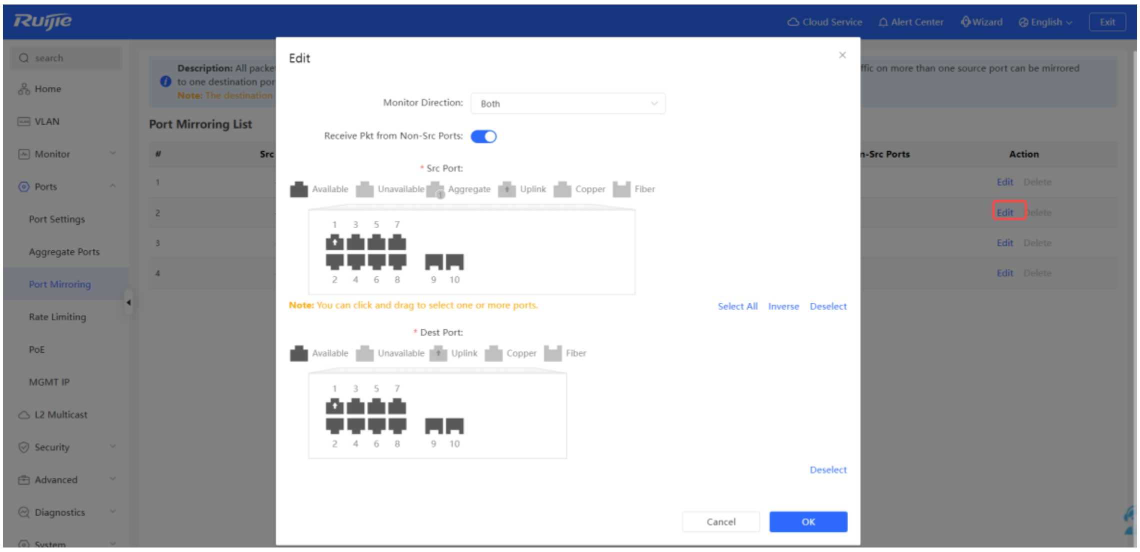
- A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.



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: On

* Src Port:

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

* Dest Port:

Table 7-4 Description of Port Mirroring Parameters

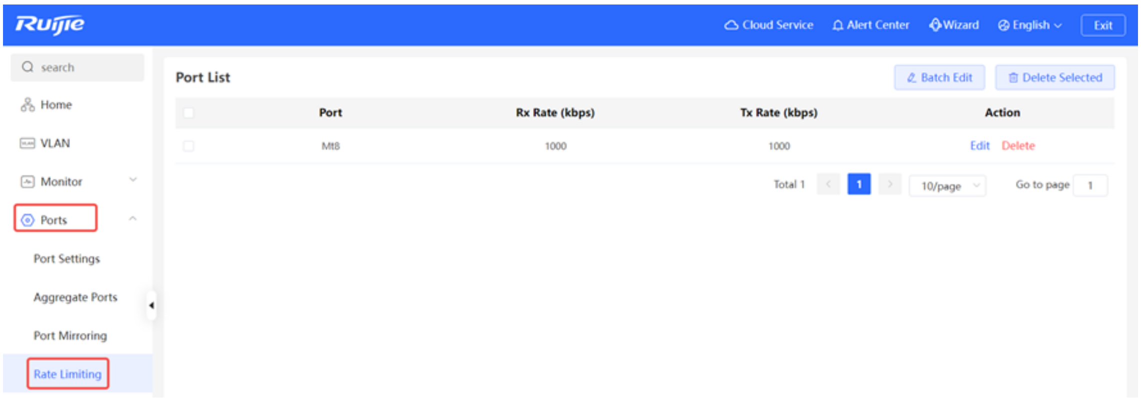
Parameter	Description	Default Value
Src Port	A source port is also called a monitored port. Data flows on the source port are monitored for network analysis or troubleshooting. Support selecting multiple source ports and mirroring multiple ports to one destination port	N/A
Dest Port	The destination port 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

Parameter	Description	Default Value
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 ● Outgoing: 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-source ports are normally forwarded ● Disabled: Only monitor source port packets	Enable

7.5 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.

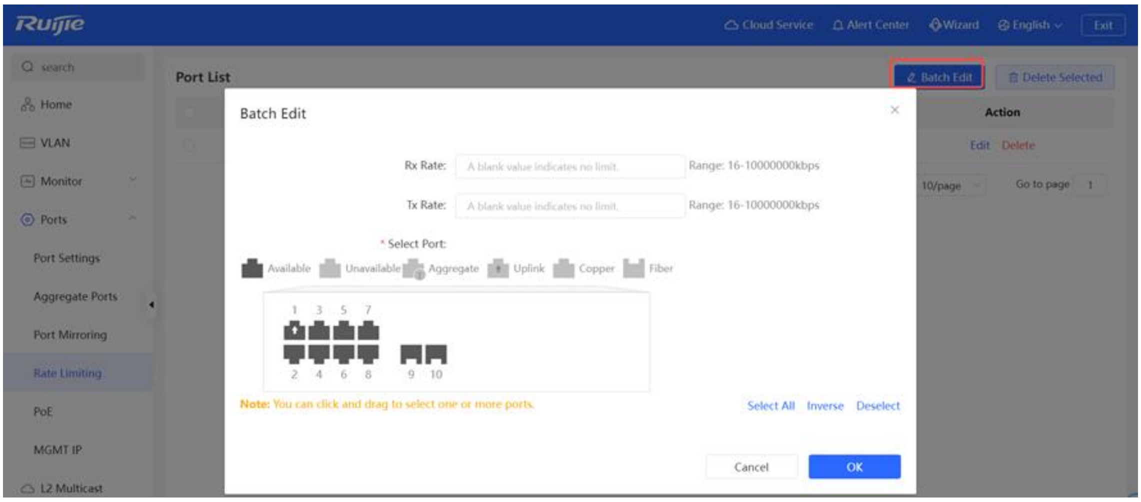


Port List

□	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
□	Mt8	1000	1000	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:

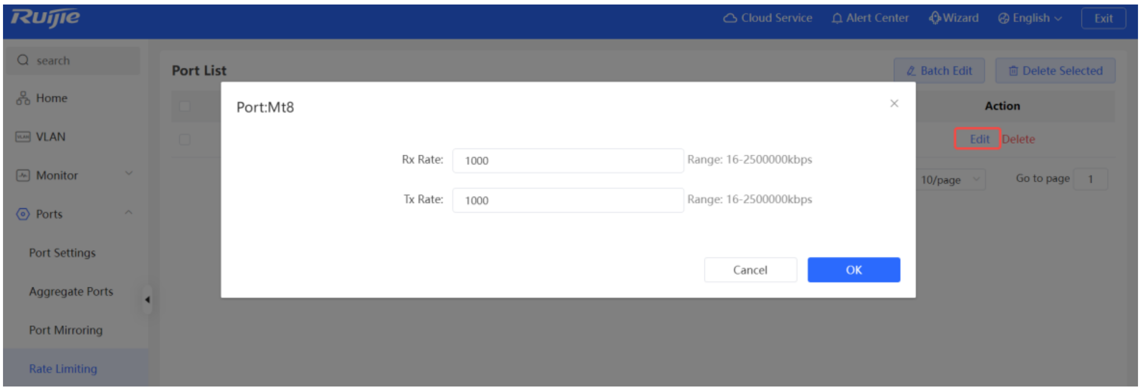
Note: You can click and drag to select one or more ports.

Table 7-5 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**.



Port:Mt8

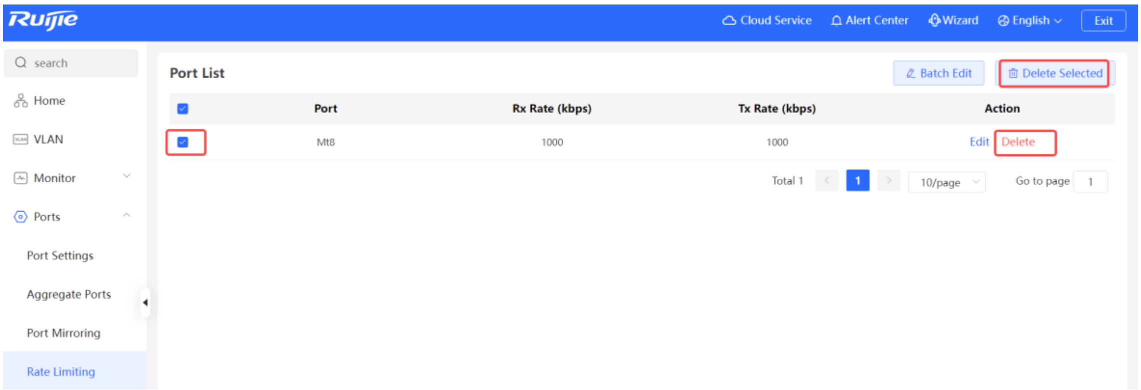
Rx Rate: 1000 Range: 16-2500000kbps

Tx Rate: 1000 Range: 16-2500000kbps

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 List

☑	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
☑	Mt8	1000	1000	Edit Delete

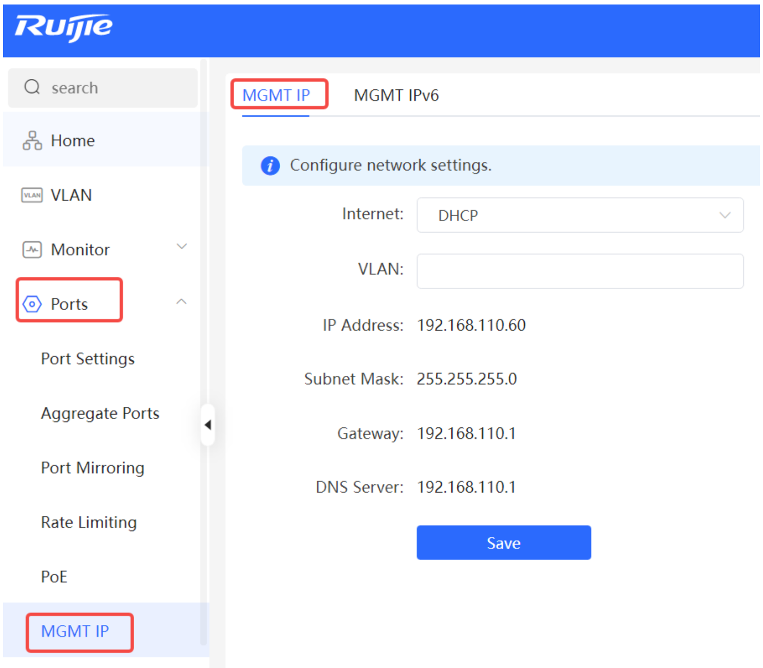
Note

- 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.

7.6 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.



Configure network settings.

Internet: DHCP

VLAN:

IP Address: 192.168.110.60

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 5.2 Configuring a VLAN).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web interface.

7.7 Configuring the Management IPv6 Address

Configure the IPv6 address used to log in to the device management page.

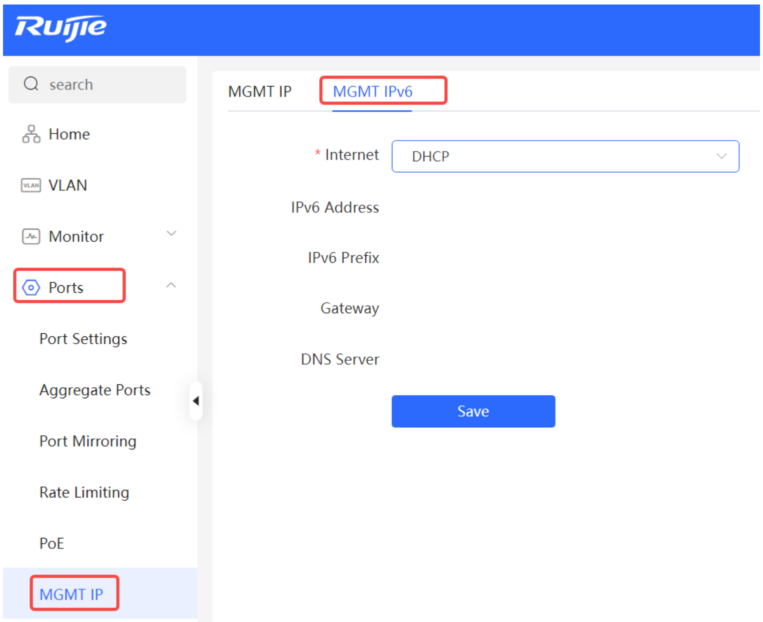
Choose **Local Device** > **Ports** > **MGMT IP** > **MGMT IPv6**.

Configure the management IPv6 address so that you can log in to the device management page using the IPv6 address of the device.

The device supports the following Internet connection types:

- **Null**: The IPv6 function is disabled on the current port.
- **DHCP**: The device dynamically obtains an IPv6 address from the upstream device.
- **Static IP**: You need to manually configure the IPv6 address, length, gateway address, and DNS server.

Click **Save**.



* Internet: DHCP

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

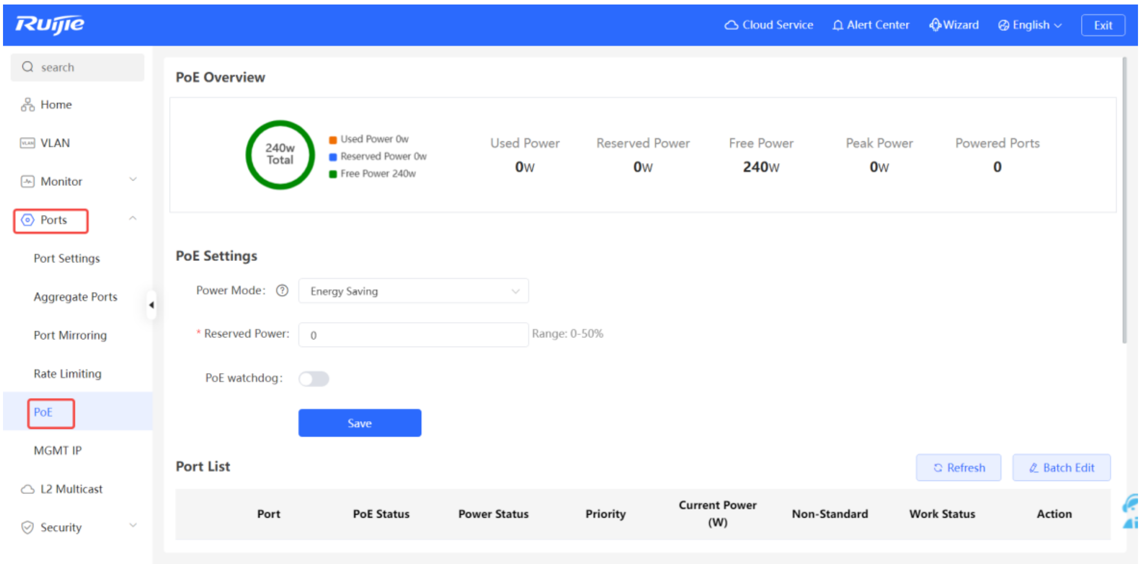
7.8 PoE Configuration

Caution

Only PoE switches (model name containing –P, -LP, -HP, and -UP) 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

Used Power 0w
Reserved Power 0w
Free Power 240w

Used Power	Reserved Power	Free Power	Peak Power	Powered Ports
0w	0w	240w	0w	0

PoE Settings

Power Mode: Energy Saving

* Reserved Power: 0 Range: 0-50%

PoE watchdog:

Port List

Port	PoE Status	Power Status	Priority	Current Power (W)	Non-Standard	Work Status	Action

7.8.1 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.

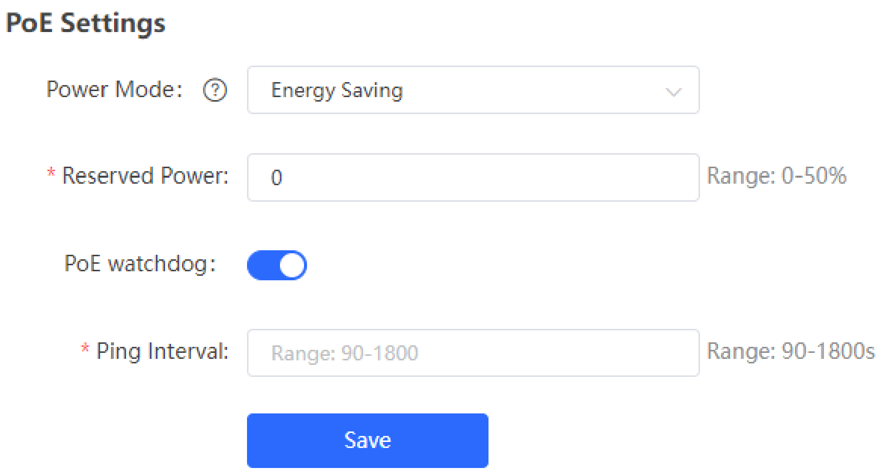
PoE watchdog: This feature is mainly applicable to security surveillance scenarios. After this feature is enabled, when a PoE port of the device suddenly stops receiving packets during the ping interval, the powered device (PD) will be restarted after the ping interval expires to restore normal operation.

Table 7-6 PoE Watchdog Configuration Description

Packet Receiving Status of the PoE Port	PoE Watchdog is Enabled	Action Taken on the PD
During the ping interval, a PoE port of the device suddenly stops receiving packets.	Yes	The PD is restarted to restore normal operation, and the ping interval is reset.
	No	No action is initiated on the PD.
During the ping interval, a PoE port of the device still stops receiving packets.	Yes	No action is initiated on the PD.
	No	No action is initiated on the PD.
During the ping interval, a PoE port of the device starts to receive packets.	Yes	The ping interval is reset.
	No	No action is initiated on the PD.

Note

If a non-PD, such as a computer, is connected to a PoE-enabled port of this device, the PoE watchdog will not initiate any action on the non-PD even if the trigger condition is met.



PoE Settings

Power Mode: Energy Saving

* Reserved Power: 0 Range: 0-50%

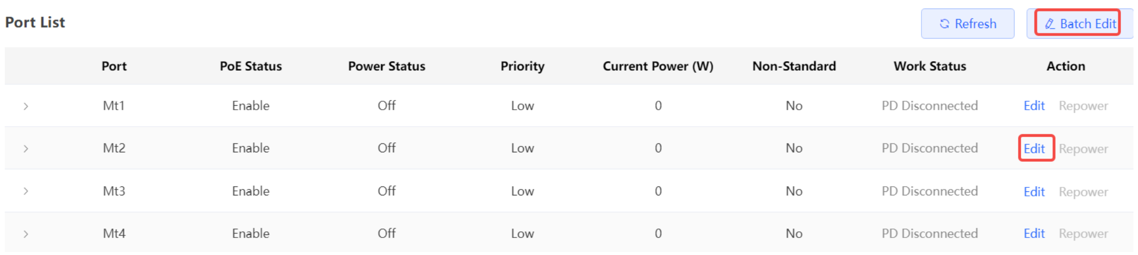
PoE watchdog: enabled

* Ping Interval: Range: 90-1800 Range: 90-1800s

7.8.2 Power Supply Configuration of Ports

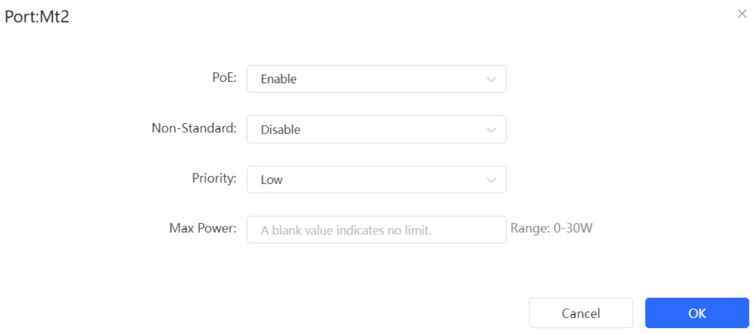
Choose **Local Device** > **Ports** > **PoE** > **Port List**.

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	Power Status	Priority	Current Power (W)	Non-Standard	Work Status	Action
›	Mt1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Mt2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Mt3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Mt4	Enable	Off	Low	0	No	PD Disconnected	Edit Repower



Port:Mt2

PoE: Enable

Non-Standard: Disable

Priority: Low

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

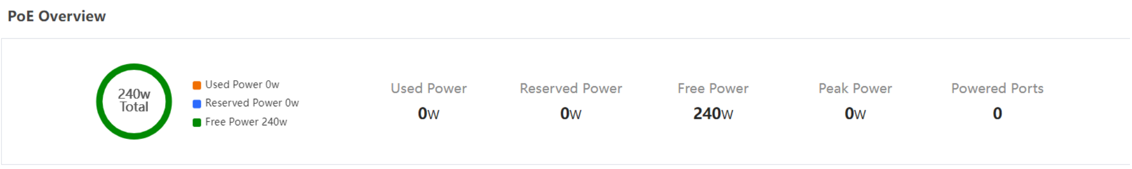
Table 7-7 Description of Parameters for Power Supply Configuration of Ports

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

7.8.3 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

240w Total

🟧 Used Power 0w
🟦 Reserved Power 0w
🟩 Free Power 240w

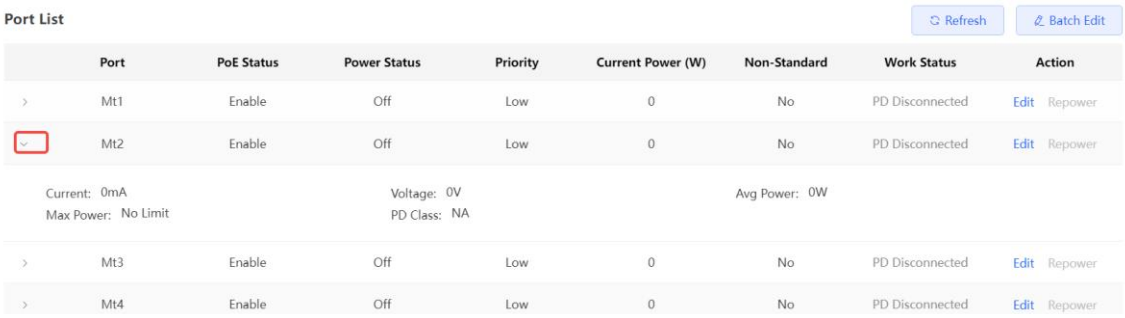
Used Power	Reserved Power	Free Power	Peak Power	Powered Ports
0w	0w	240w	0w	0

7.8.4 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 List

Refresh Batch Edit

	Port	PoE Status	Power Status	Priority	Current Power (W)	Non-Standard	Work Status	Action
›	Mt1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
⌄	Mt2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Current: 0mA Voltage: 0V Avg Power: 0W
Max Power: No Limit PD Class: NA

	Port	PoE Status	Power Status	Priority	Current Power (W)	Non-Standard	Work Status	Action
›	Mt3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
›	Mt4	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Table 7-8 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 supplies 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).

Field	Description
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.

8 L2 Multicast

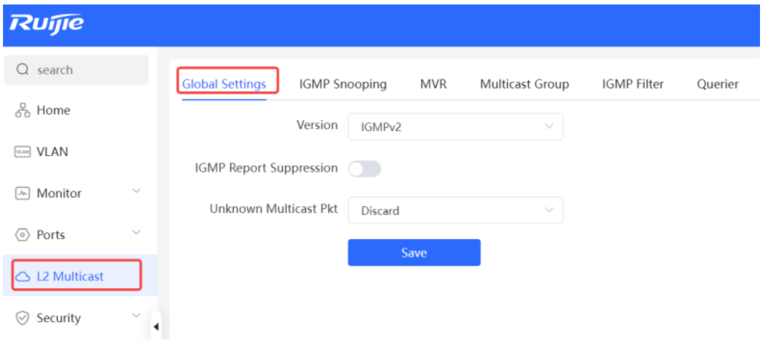
8.1 Multicast Overview

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.

8.2 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 8-1 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, and 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

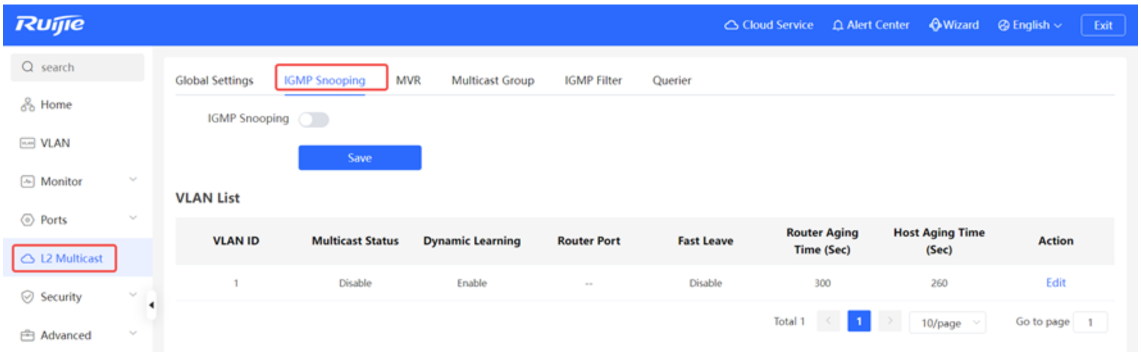
Parameter	Description	Default Value
IGMP Report Suppression	After this function is enabled, to reduce the number of packets on the network, save network bandwidth and ensure the performance of the IGMP multicast device, the switch forwards only one report packet to the multicast router if multiple downlink 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

8.3 IGMP Snooping

8.3.1 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, a 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.



IGMP Snooping ○

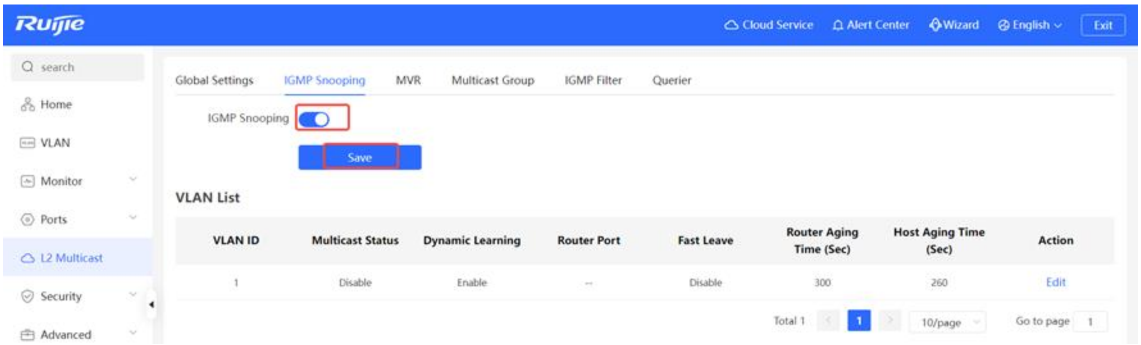
VLAN List

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

8.3.2 Enabling Global IGMP Snooping

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

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



IGMP Snooping: ●

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

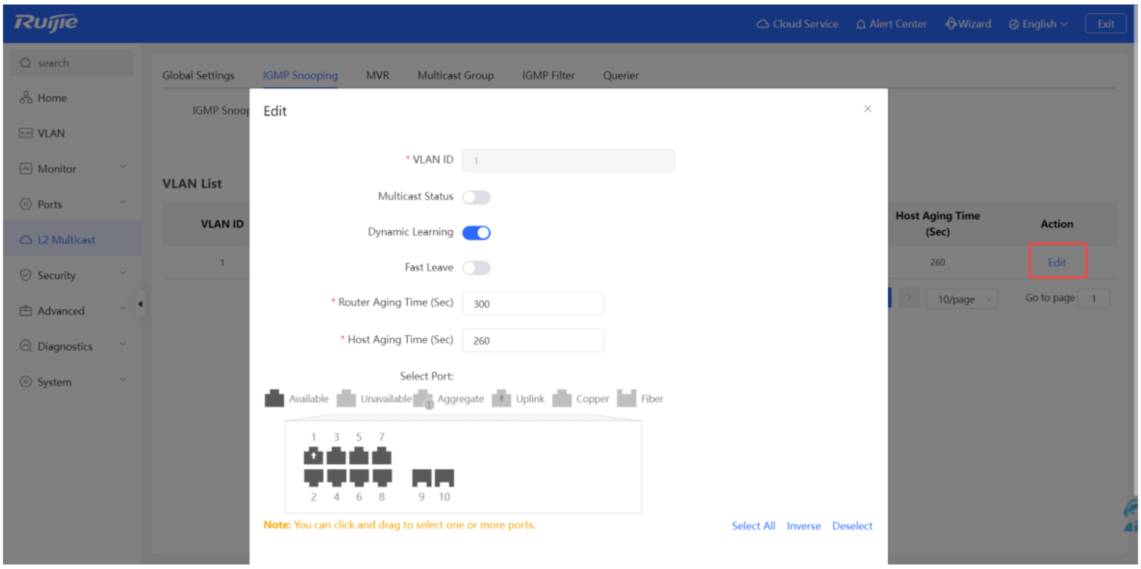
8.3.3 Configuring Protocol Packet Processing Parameters

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**.



Edit

* VLAN ID: 1

Multicast Status: ○

Dynamic Learning: ●

Fast Leave: ○

* 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 8-2 Description of VLAN Configuration Parameters of IGMP Snooping

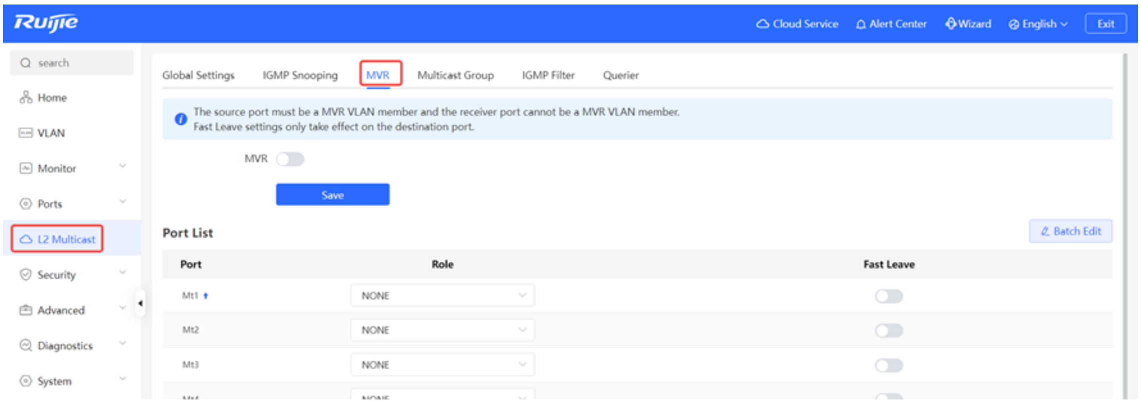
Parameter	Description	Default Value
Multicast Status	Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled.	Disable

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.	N/A
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	N/A

8.4 Configuring MVR

8.4.1 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.



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

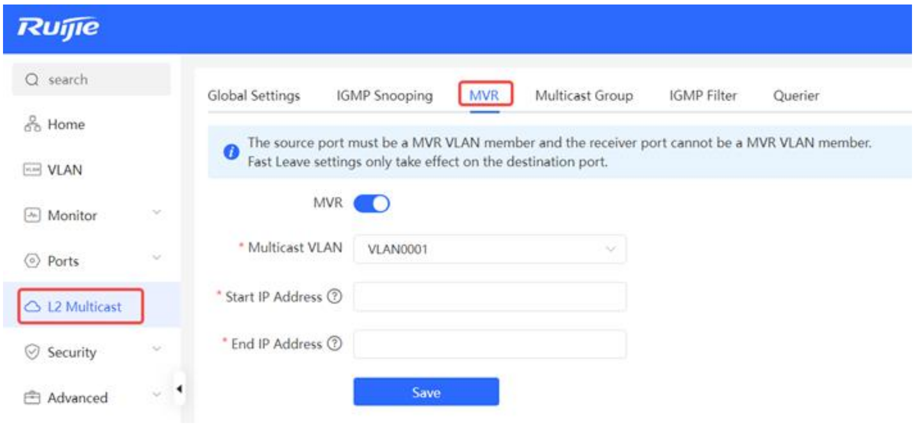
Port List

Port	Role	Fast Leave
Mt1	NONE	
Mt2	NONE	
Mt3	NONE	

8.4.2 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.



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

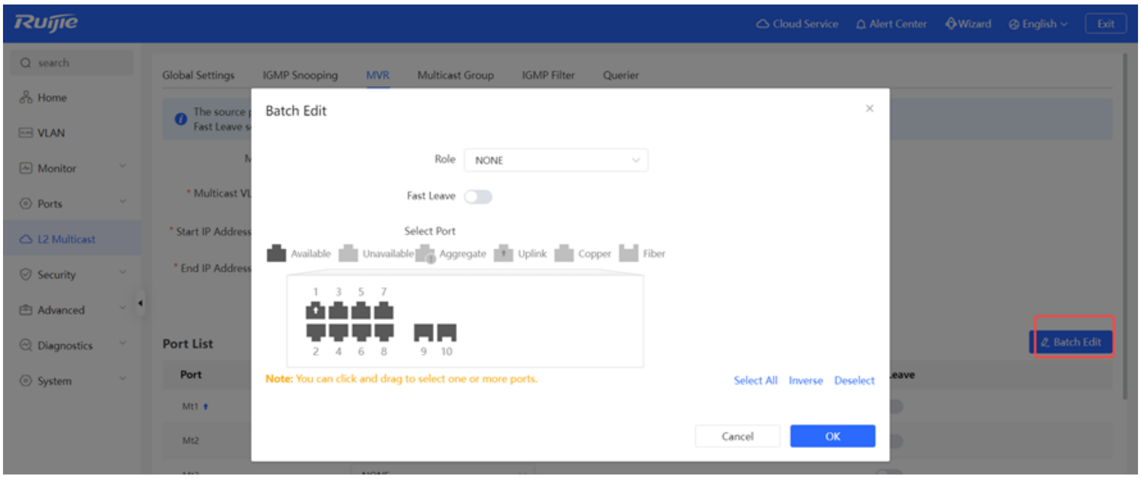
Table 8-3 **Description of Configuring Global MVR Parameters**

Parameter	Description	Default Value
MVR	Enables/Disables MVR globally	Disable
Multicast VLAN	VLAN of a multicast source	1
Start IP Address	Learned or configured start multicast IP address of an MVR multicast group.	N/A
End IP Address	Learned or configured end multicast IP address of an MVR multicast group.	N/A

8.4.3 Configuring the MVR Ports

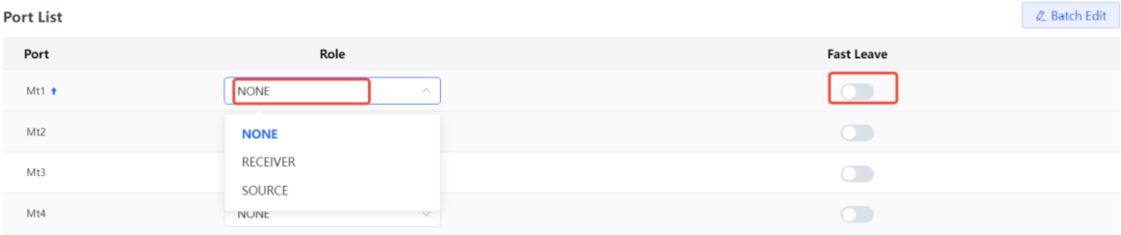
Choose **Local Device** > **L2 Multicast** > **MVR**.

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**.



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	Role	Fast Leave
Mt1	NONE	
Mt2		
Mt3		
Mt4	NONE	

Table 8-4 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.

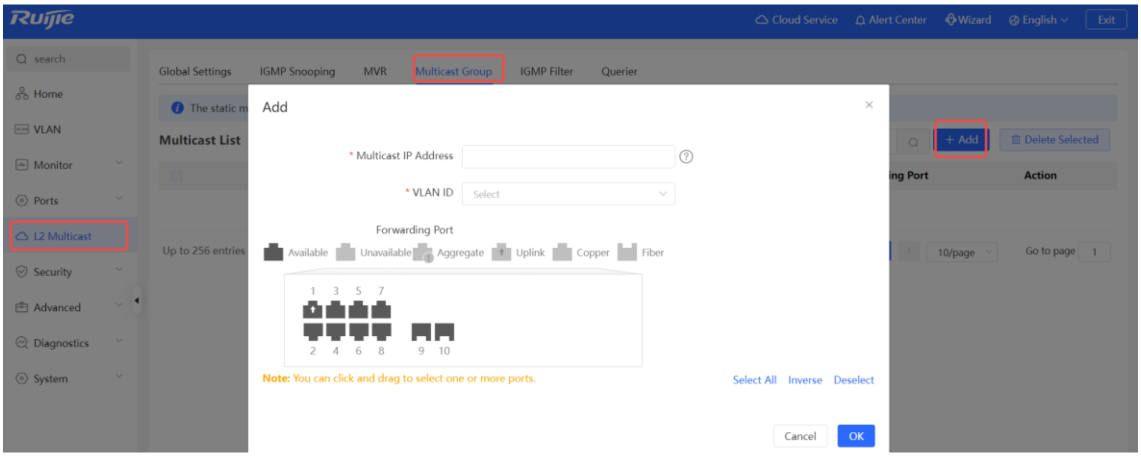
8.5 Configuring Multicast Group

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.



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

Table 8-5 Description of Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	N/A
Multicast IP Address	On-demand multicast IP address	N/A
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.	N/A
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.	N/A
Forwarding Port	List of ports that forward multicast traffic	N/A

Note

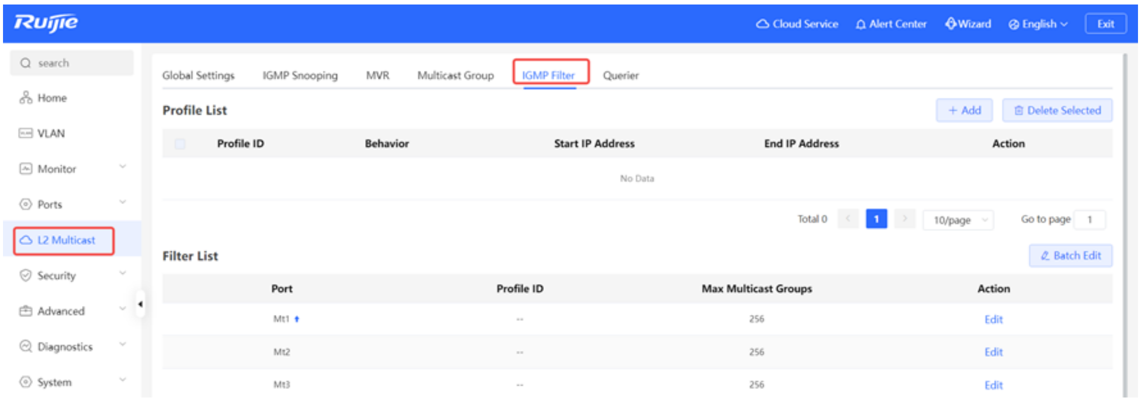
Static multicast groups cannot learn other dynamic forwarding ports.

8.6 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				

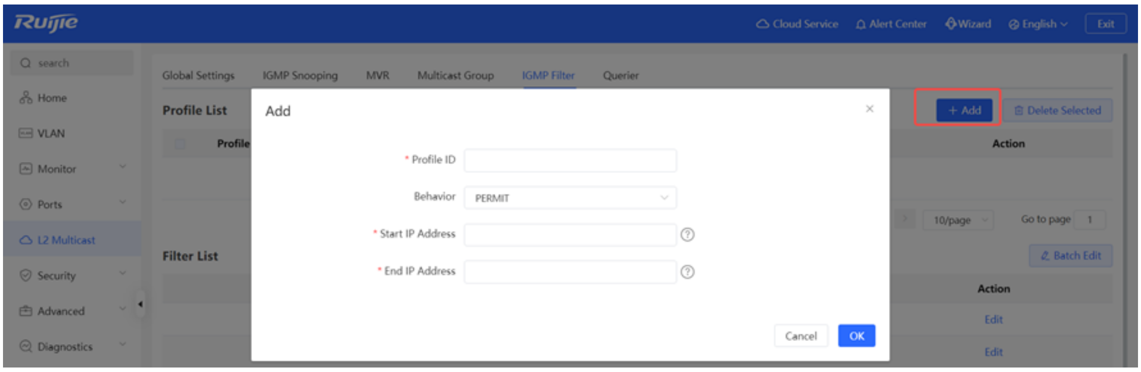
Filter List

Port	Profile ID	Max Multicast Groups	Action
Mt1	--	256	Edit
Mt2	--	256	Edit
Mt3	--	256	Edit

8.6.1 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.



Add

* Profile ID

Behavior: PERMIT

* Start IP Address

* End IP Address

Table 8-6 **Description of Profile Configuration Parameters**

Parameter	Description	Default Value
Profile ID	Profile ID	N/A

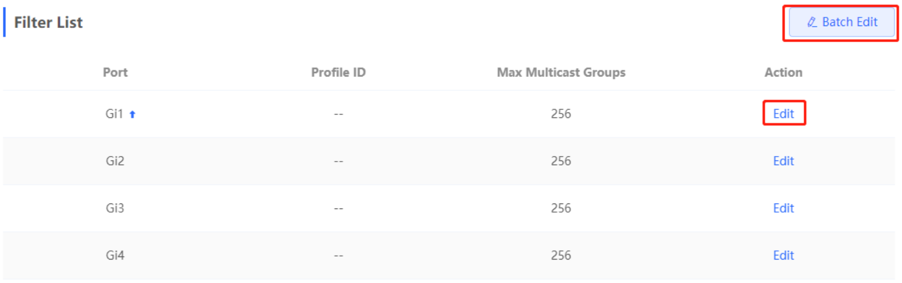
Parameter	Description	Default Value
Behavior	**DENY**: Forbids demanding multicast IP addresses in a specified range. **PERMIT**: Only allows demanding multicast IP addresses in a specified range.	N/A
Start IP Address	Start Multicast IP address of the range of multicast group addresses	N/A
End IP Address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

8.6.2 Configuring a Range of Multicast Groups for a Profile

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

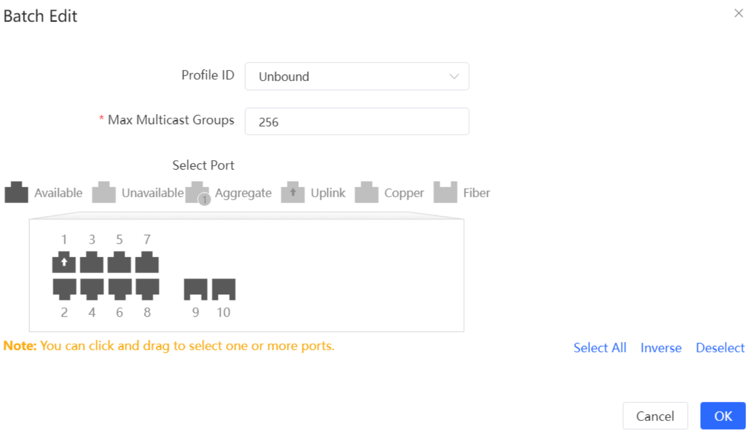
The port filter can cite a profile to define the range of multicast group addresses that can be or cannot be demanded by users on a port.

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

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 8-7 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.	N/A
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

8.7 Setting an IGMP Querier

8.7.1 Overview

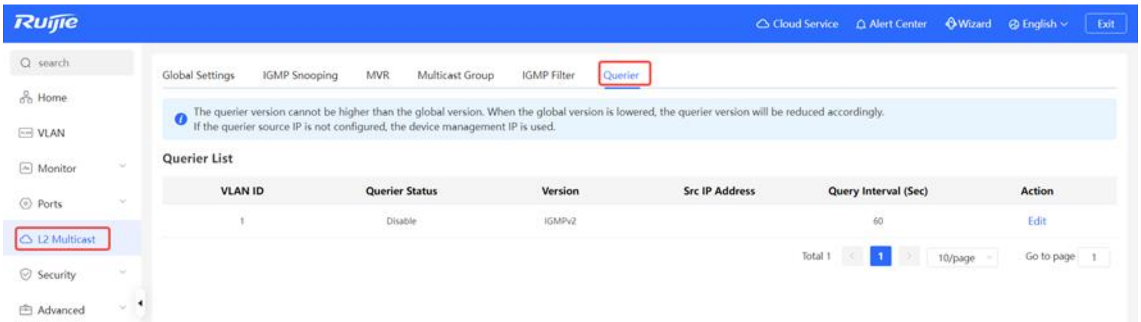
In a three-layer multicast network, the L3 multicast device serves as the querier and runs IGMP to maintain group membership. L2 multicast devices only need to listen to IGMP packets to establish and maintain forwarding entries and implement L2 multicasting. When a multicast source and user host are 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.

8.7.2 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.

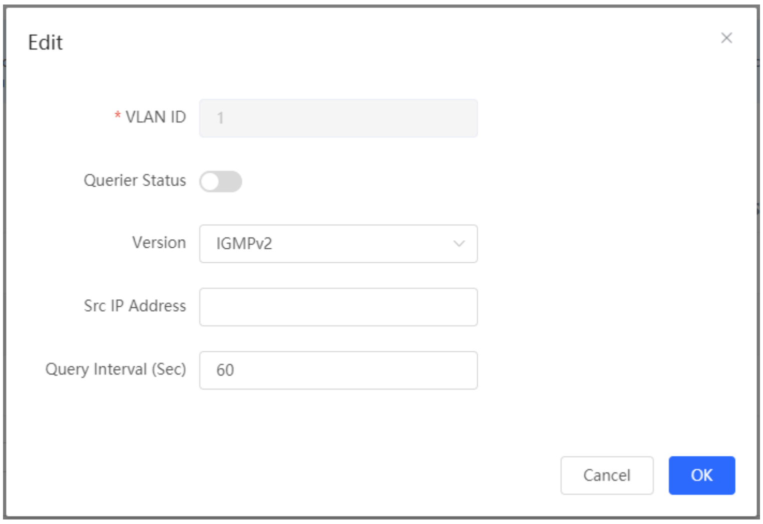
In **Querier List**, click **Edit** in the **Action** column. In the displayed dialog box, select whether to enable the querier, set the querier version, querier source IP address, and packet query interval, and click **OK**.



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



Edit

* VLAN ID: 1

Querier Status: ○

Version: IGMPv2

Src IP Address:

Query Interval (Sec): 60

Table 8-8 **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.	N/A
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.

9 Security

9.1 DHCP Snooping

9.1.1 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.

9.1.2 Standalone Device Configuration

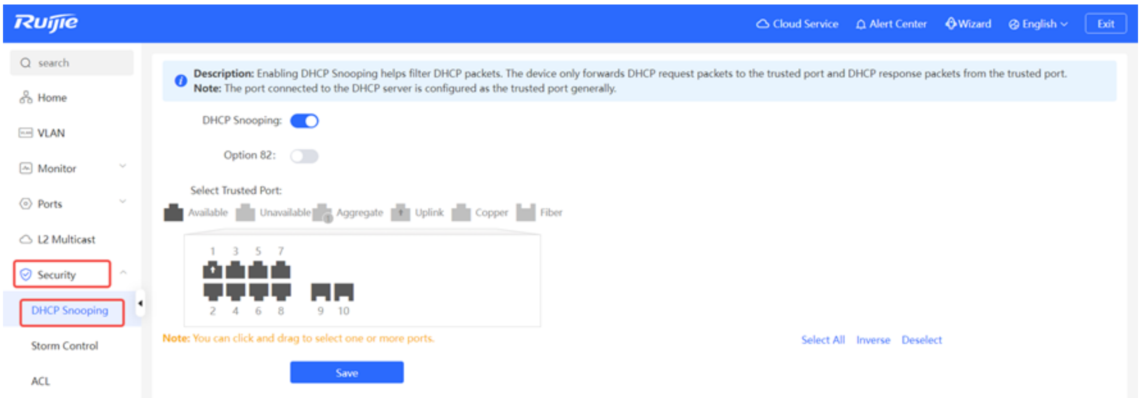
Choose **Local Device** > **Security** > **DHCP Snooping**.

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.



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:

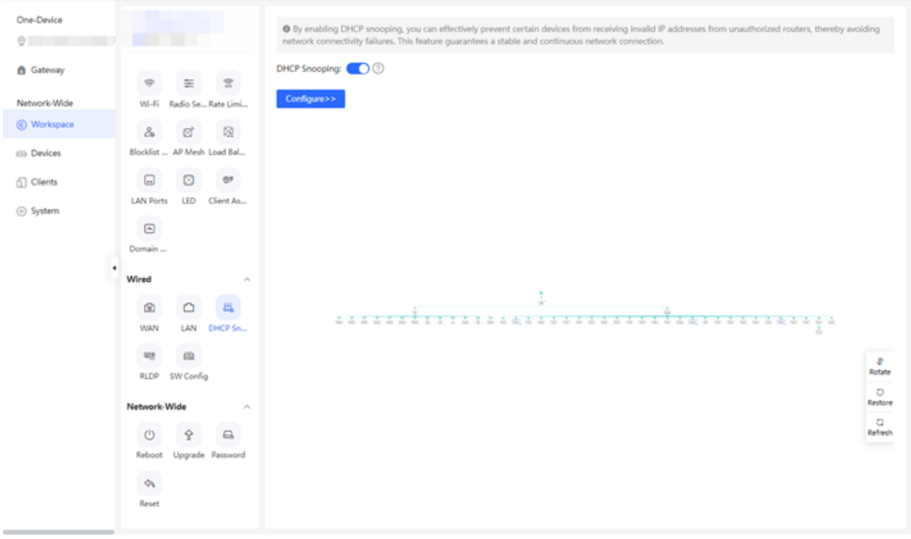
Note: You can click and drag to select one or more ports.

9.1.3 Batch Configuring Network Switches

Choose **Network-Wide** > **Workspace** > **Wired** > **DHCP Snooping**.

Enabling DHCP Snooping on network switches can ensure that users can only obtain network configuration parameters from the DHCP server within the control range, and avoid a host on the original network obtaining an IP address assigned by an unauthorized router, so as to guarantee the stability of the network.

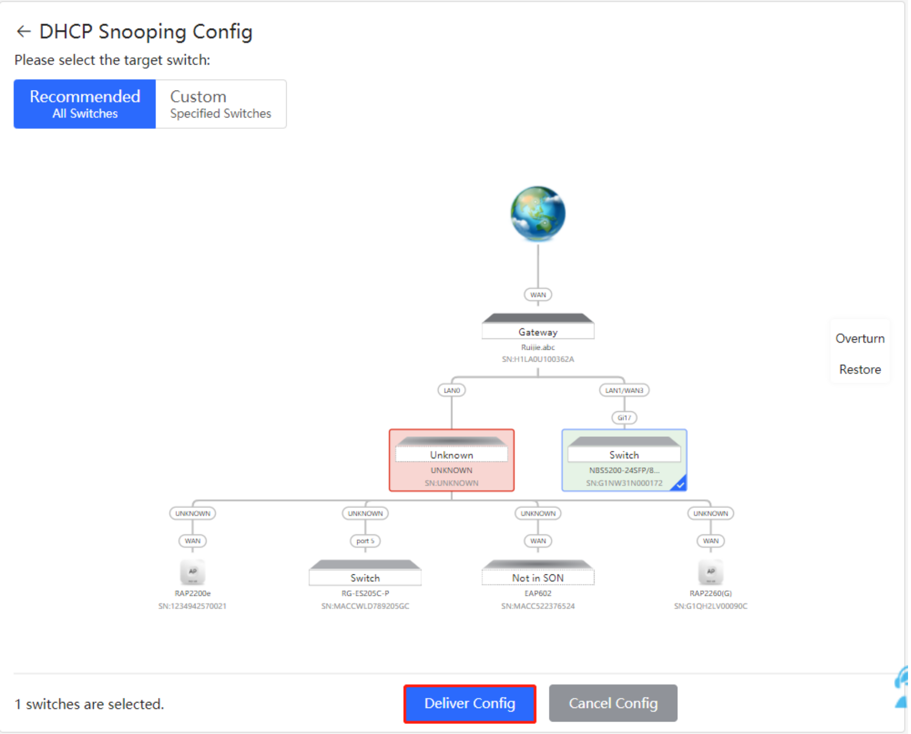
(1) Click **Enable** to access the **DHCP Snooping Config** page.



By enabling DHCP snooping, you can effectively prevent certain devices from receiving invalid IP addresses from unauthorized routers, thereby avoiding network connectivity failures. This feature guarantees a stable and continuous network connection.

DHCP Snooping: ● ⓘ

(2) On 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 on 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.

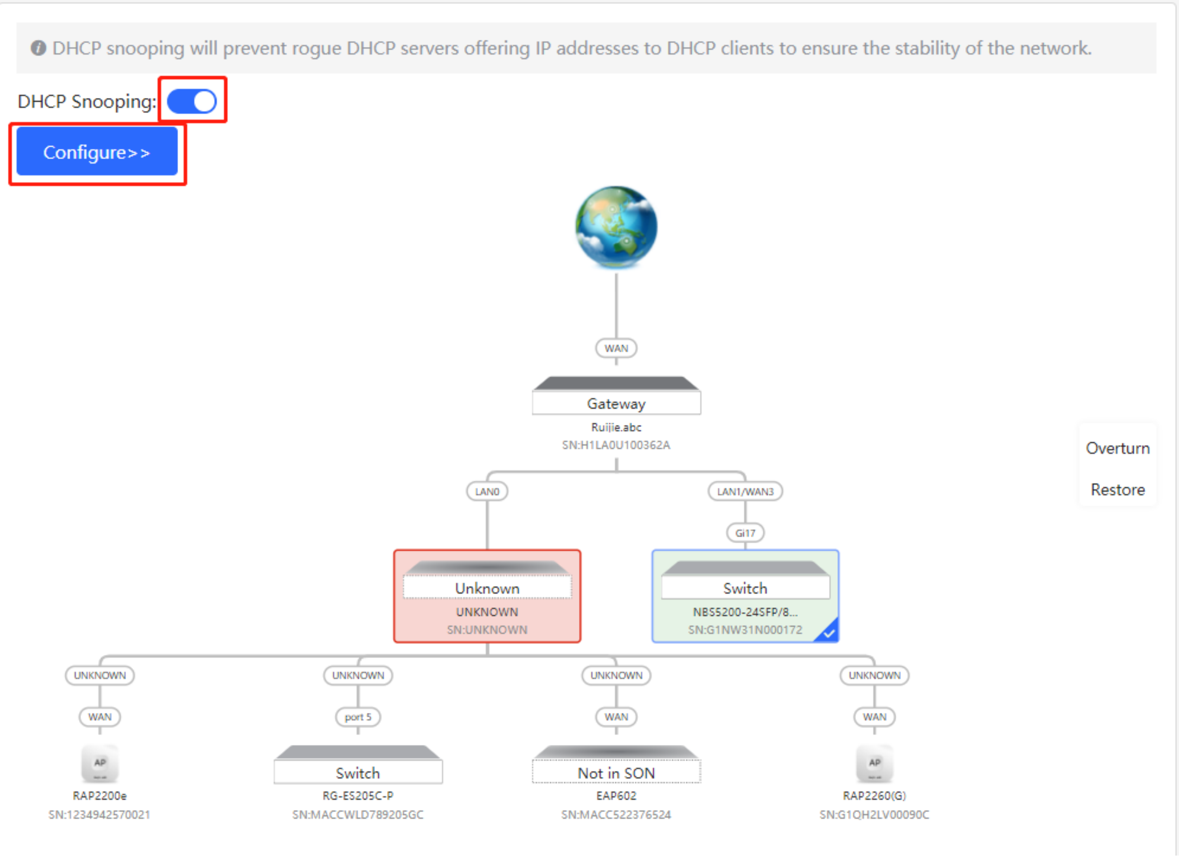


← DHCP Snooping Config

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: ●

9.2 Storm Control

9.2.1 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.

9.2.2 Procedure

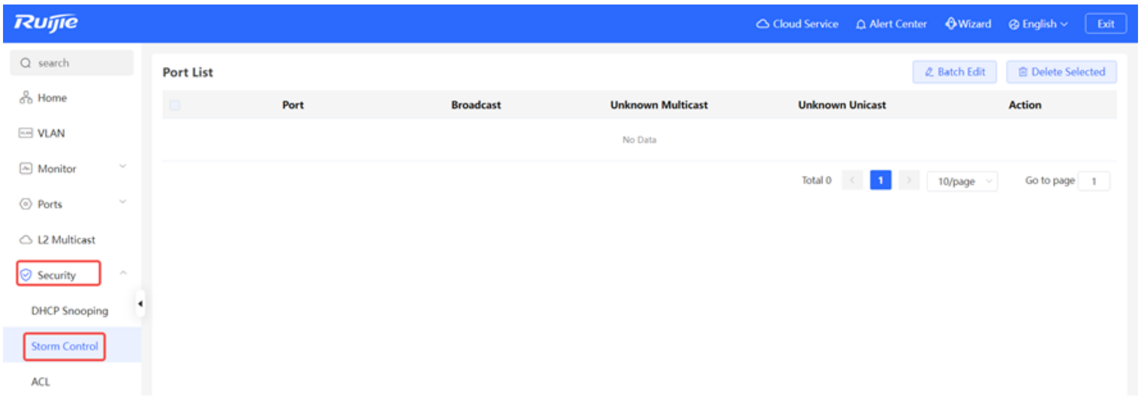
Choose **Local Device** > **Security** > **Storm Control**.

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.

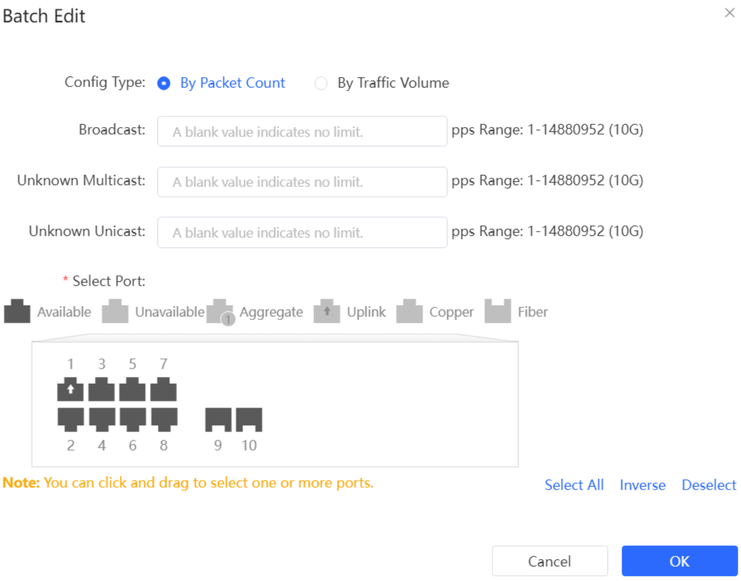
- Storm control based on kilobytes per second: If the rate of data flows received over a device port exceeds the configured kilobytes-per-second threshold, excess data flows are discarded until the rate falls within the threshold.



Port List

Port	Broadcast	Unknown Multicast	Unknown Unicast	Action

No Data



Batch Edit

Config Type: ● By Packet Count ○ By Traffic Volume

Broadcast: A blank value indicates no limit. pps Range: 1-14880952 (10G)

Unknown Multicast: A blank value indicates no limit. pps Range: 1-14880952 (10G)

Unknown Unicast: A blank value indicates no limit. pps Range: 1-14880952 (10G)

* Select Port:

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

9.3 ACL

9.3.1 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.

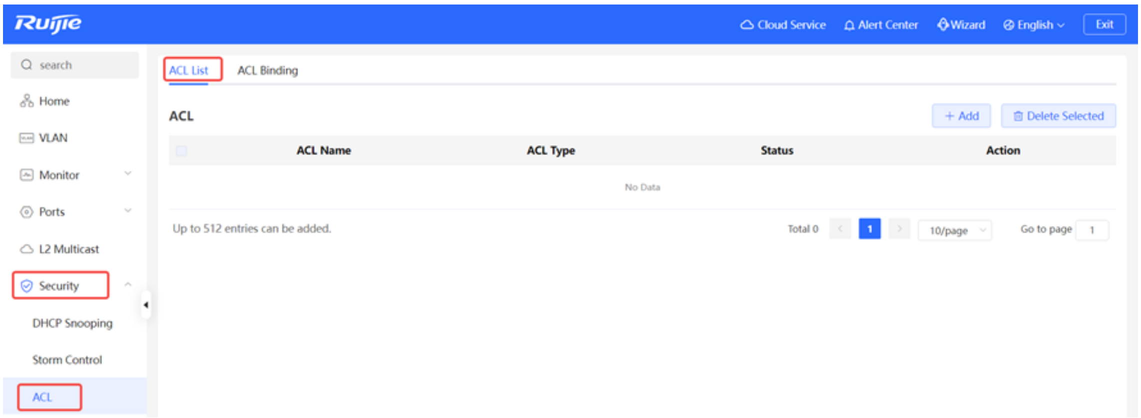
9.3.2 Creating ACL Rules

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.



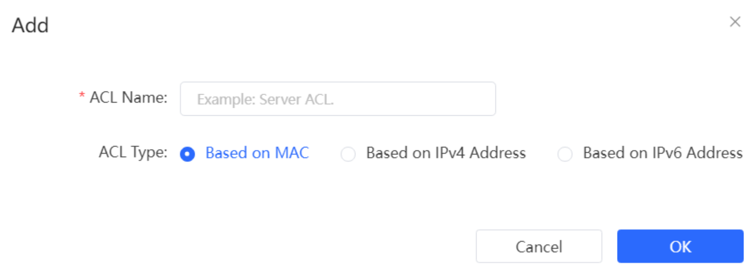
ACL

☐	ACL Name	ACL Type	Status	Action

No Data

Up to 512 entries can be added.

Total 0 < 1 > 10/page Go to page 1

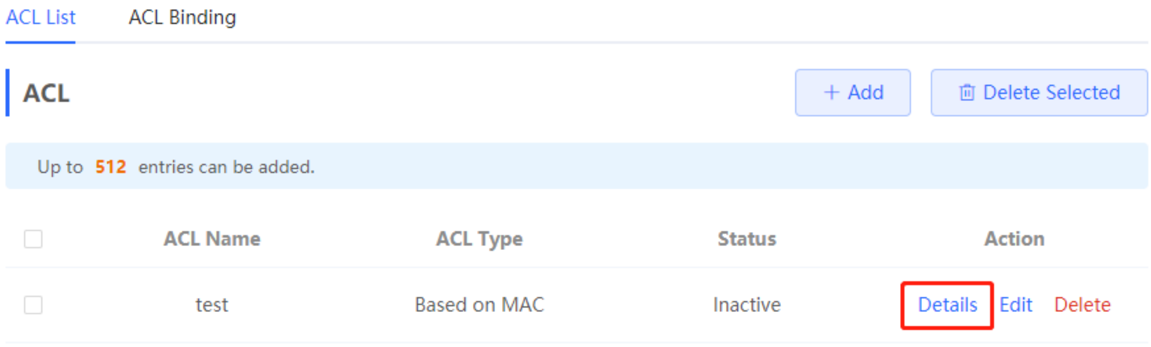


* ACL Name: Example: Server ACL

ACL Type: ● Based on MAC ○ Based on IPv4 Address ○ Based on IPv6 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.

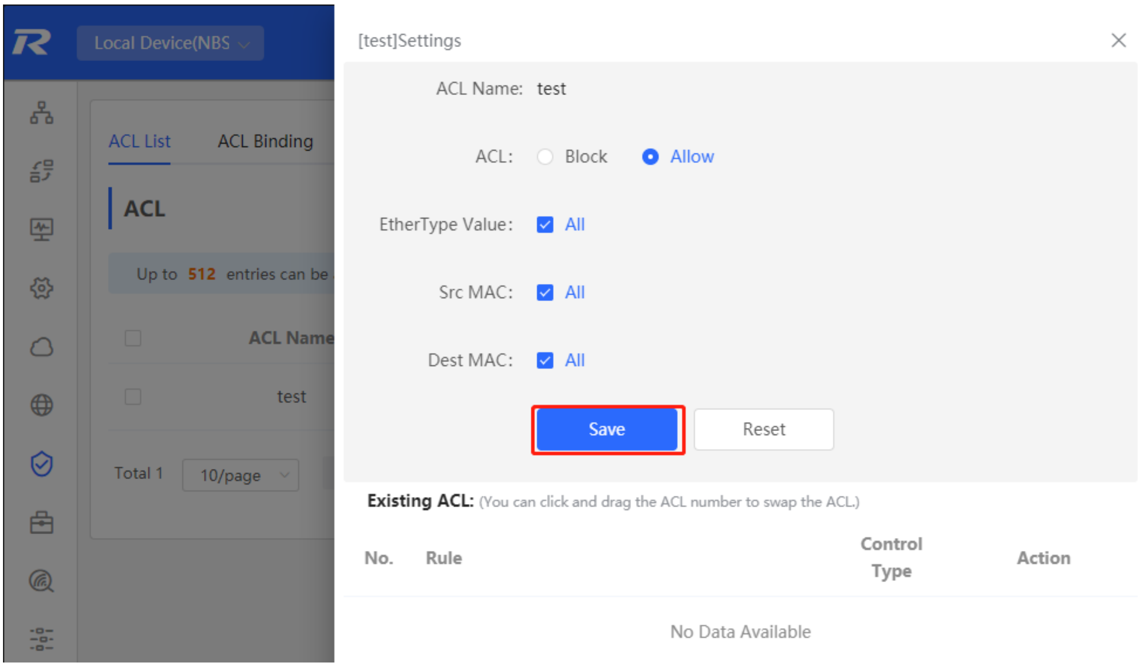
The rules include two actions of **Allow** or **Block**, and the matching rules of packets. The sequence of a Rule in an ACL determines the matching priority of the Rule in the ACL. When processing packets, the network device matches packets with ACEs based on the Rule sequence numbers. Click **Move**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



ACL

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

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

No.	Rule	Control Type	Action
No Data Available			

Table 9-1 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.

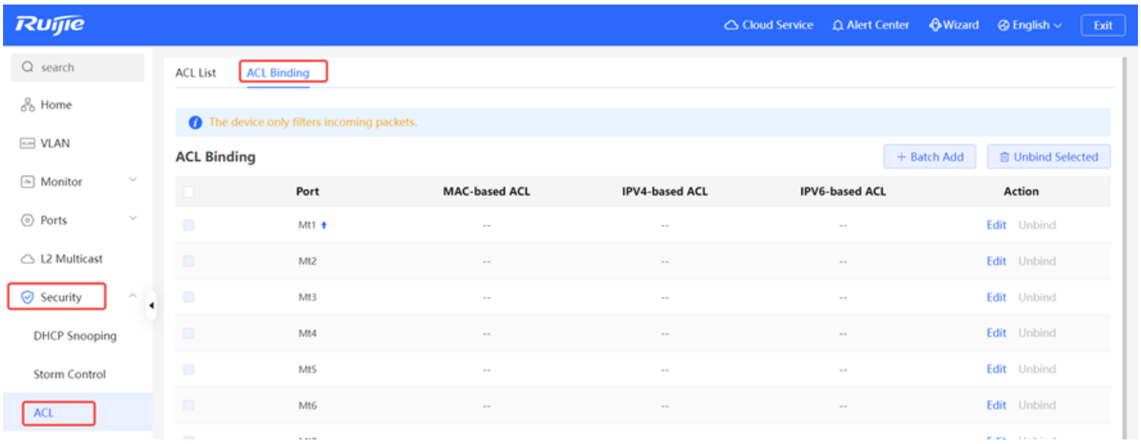
9.3.3 Applying ACL Rules

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.

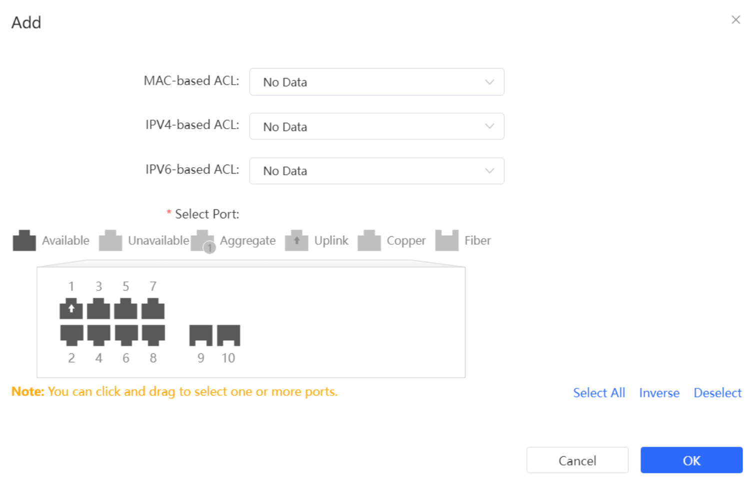


The device only filters incoming packets.

ACL Binding

+ Batch Add | Unbind Selected

□	Port	MAC-based ACL	IPV4-based ACL	IPV6-based ACL	Action
□	Mt1	--	--	--	Edit Unbind
□	Mt2	--	--	--	Edit Unbind
□	Mt3	--	--	--	Edit Unbind
□	Mt4	--	--	--	Edit Unbind
□	Mt5	--	--	--	Edit Unbind
□	Mt6	--	--	--	Edit Unbind



MAC-based ACL: No Data

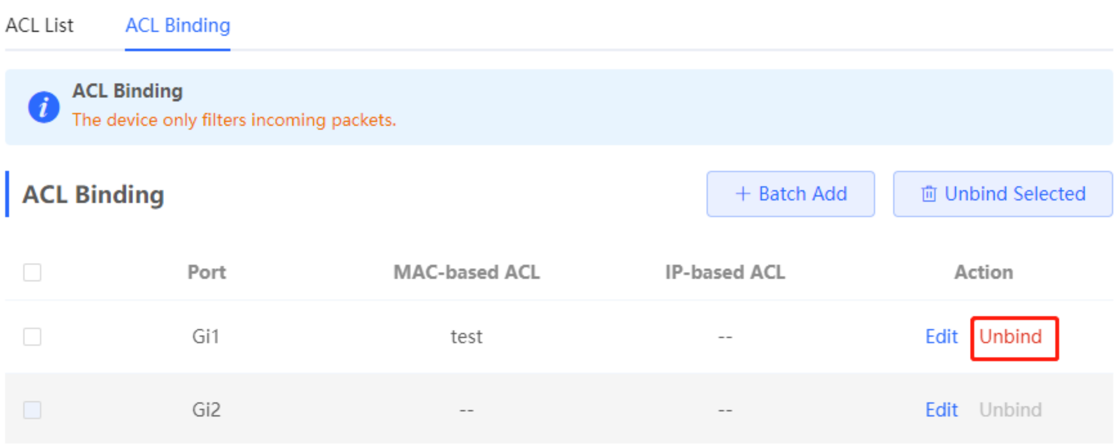
IPV4-based ACL: No Data

IPV6-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

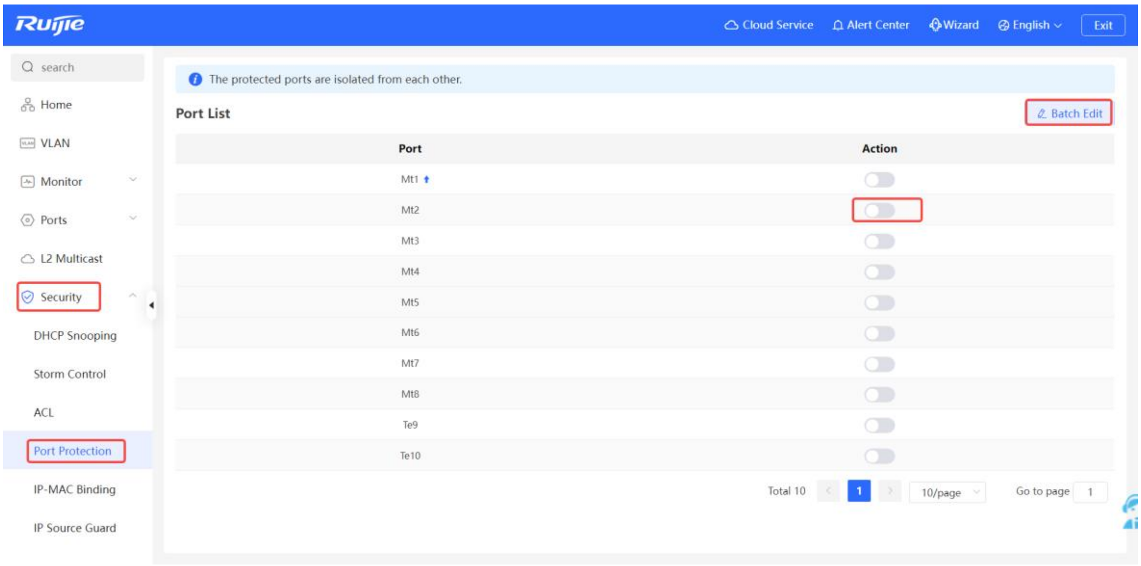
□	Port	MAC-based ACL	IP-based ACL	Action
□	Gi1	test	--	Edit Unbind
□	Gi2	--	--	Edit Unbind

9.4 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.**



The protected ports are isolated from each other.

Port List

Port	Action
Mt1 ⬆	○
Mt2	○
Mt3	○
Mt4	○
Mt5	○
Mt6	○
Mt7	○
Mt8	○
Te9	○
Te10	○

9.5 IP-MAC Binding

9.5.1 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.

9.5.2 Procedure

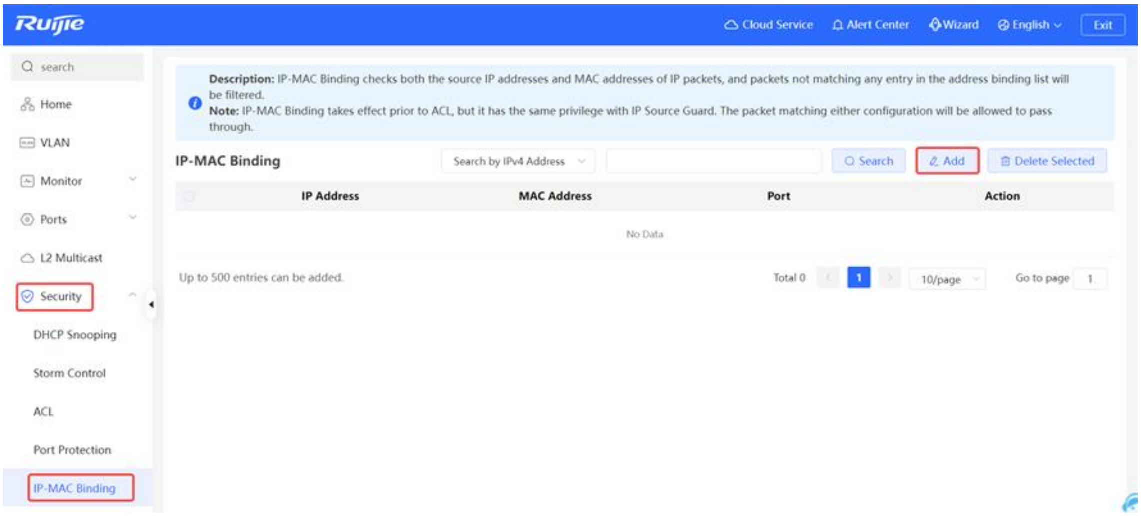
Choose **Local Device** > **Security** > **IP-MAC Binding**.

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.

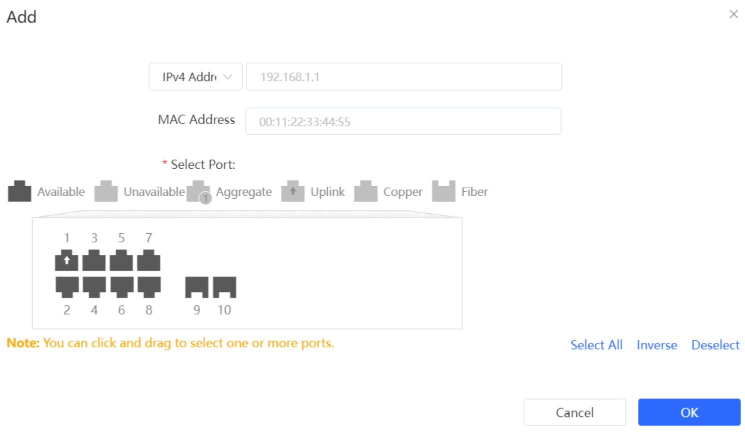


Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding list will be filtered.
Note: IP-MAC Binding takes effect prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.

IP-MAC Binding

IP Address	MAC Address	Port	Action
No Data			

Up to 500 entries can be added.



Add

IPv4 Addr 192.168.1.1

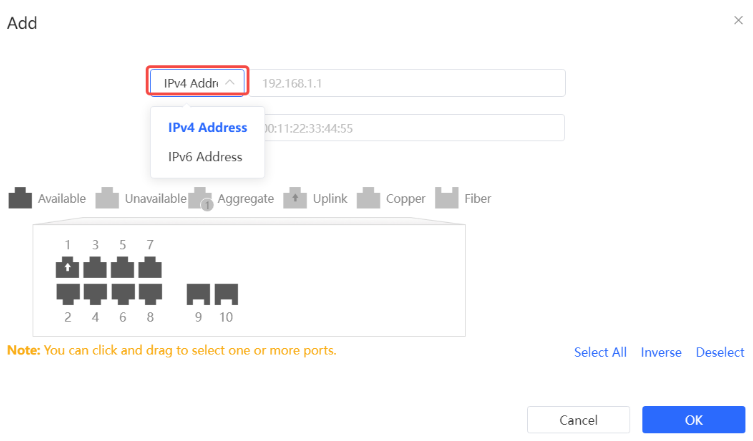
MAC Address 00:11:22:33:44:55

* 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.



192.168.1.1

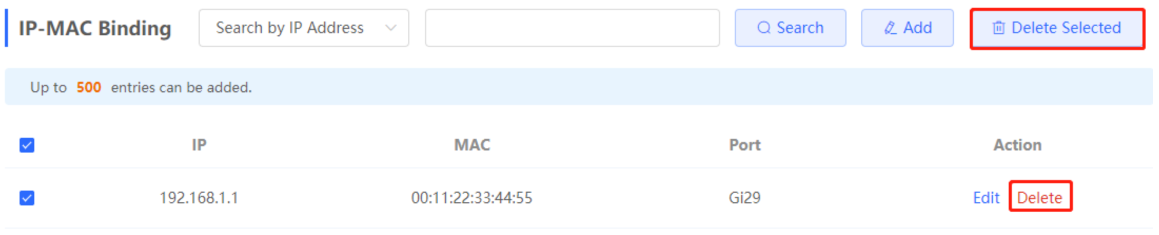
00:11:22:33:44:55

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

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 **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

9.6 IP Source Guard

9.6.1 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**

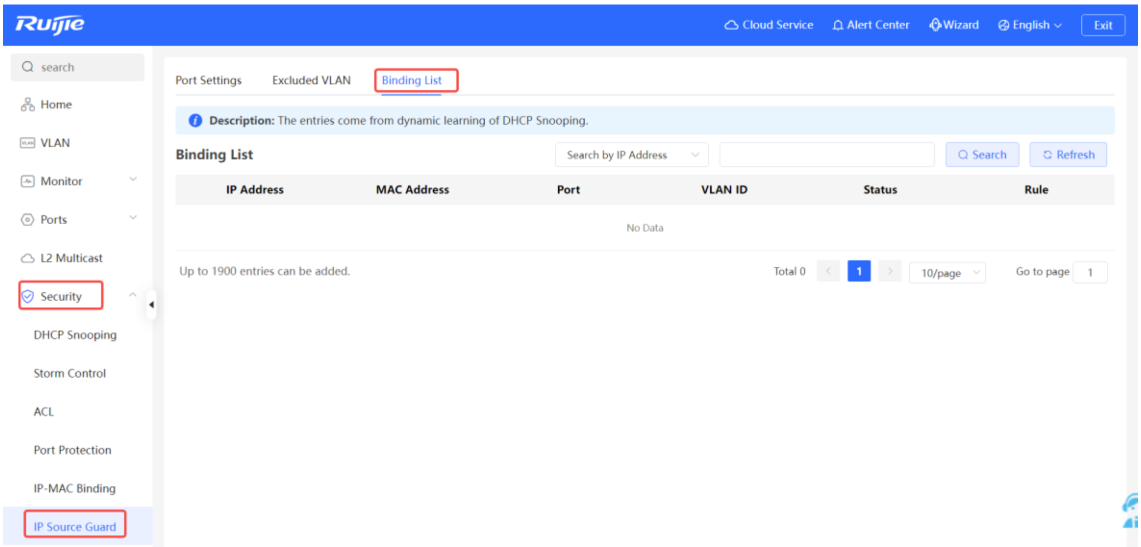
IP Source Guard should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see 7.1 for details.

9.6.2 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**.



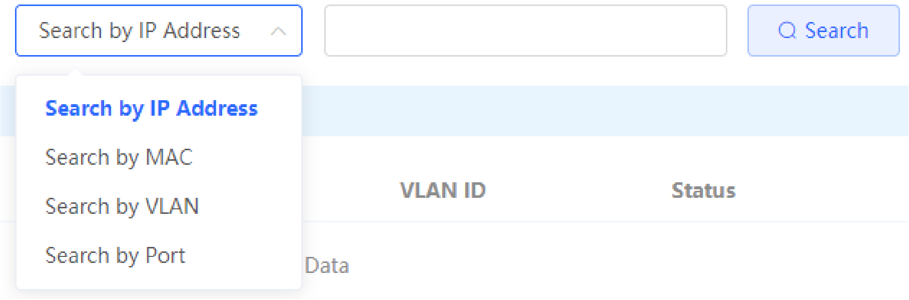
Description: The entries come from dynamic learning of DHCP Snooping.

Binding List

IP Address	MAC Address	Port	VLAN ID	Status	Rule
No Data					

Up to 1900 entries can be added.

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**.



9.6.3 Enabling Port IP Source Guard

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

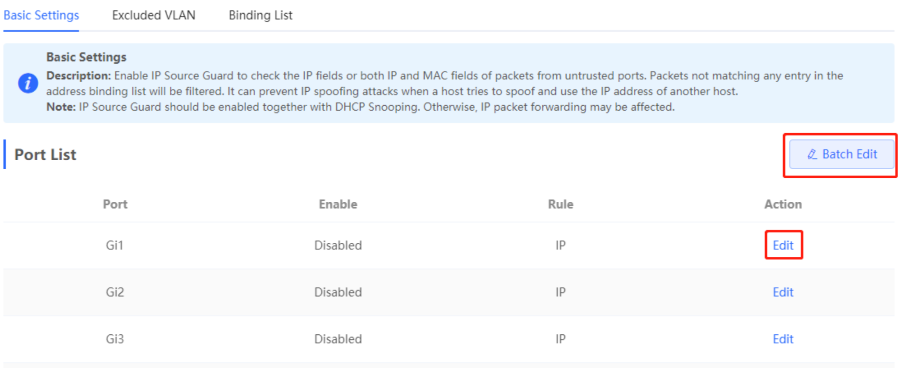
In Port List, click **Edit** in the **Action** column. Select **Enabled** and select the match rule, and click **OK**.

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 | Excluded VLAN | Binding List

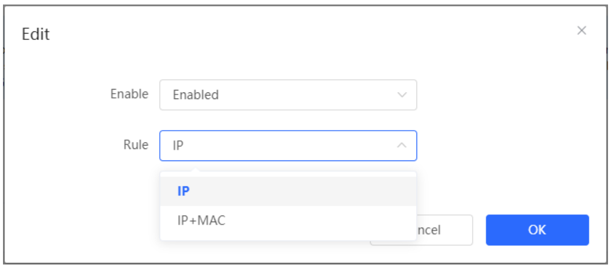
Basic Settings

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

9.6.4 Configuring Exceptional VLAN Addresses

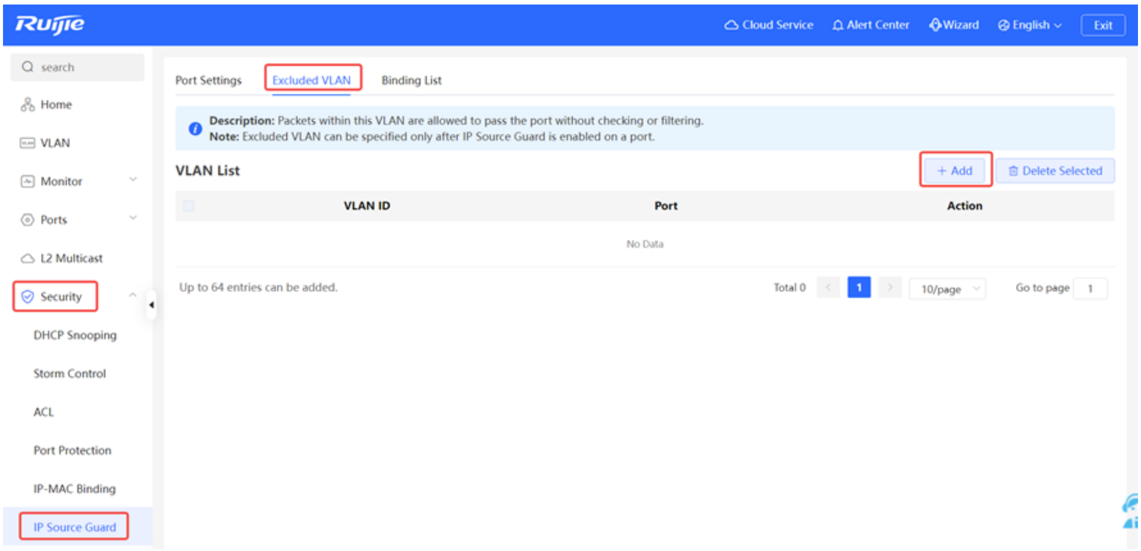
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

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.



Port Settings | Excluded VLAN | Binding List

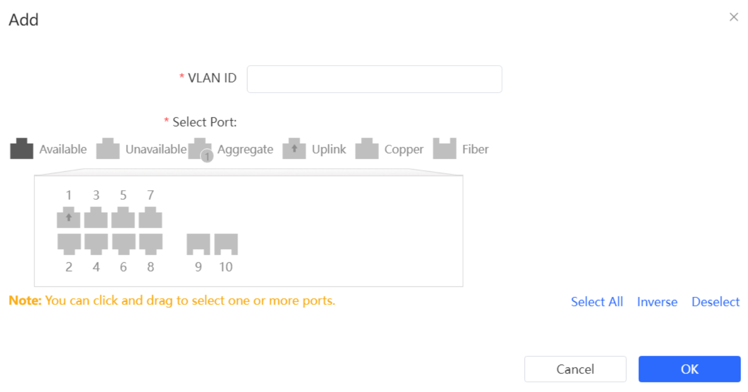
Description: Packets within this VLAN are allowed to pass the port without checking or filtering.

Note: Excluded VLAN can be specified only after IP Source Guard is enabled on a port.

VLAN List

VLAN ID	Port	Action
No Data		

Up to 64 entries can be added.


Add

* VLAN ID

* Select Port:

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

9.7 Configure 802.1x authentication

9.7.1 Function introduction

IEEE802.1x (Port-Based Network Access Control) is a port-based network access control standard that provides secure access services for LANs.

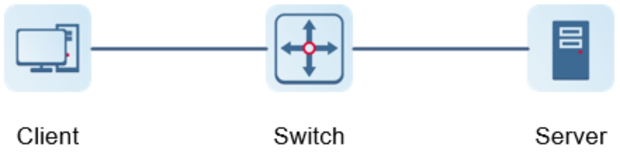
IEEE 802 LAN, as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

802.1x supports Authentication, Authorization, and Accounting three security applications, referred to as AAA.

- Authentication: Authentication, used to determine whether users can obtain access rights and restrict illegal users;
- Authorization: Authorization, which services authorized users can use, and control the rights of legitimate users;
- Accounting: Accounting, recording the use of network resources by users, and providing a basis for charging.

802.1x can be deployed in a network that controls access users to implement authentication and authorization services for access users.

802.1x system is a typical Client/Server structure, including three entities: client, access device and authentication server. A typical architecture diagram is shown in the figure.



- The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL).
- AP or switching device) that supports the 802.1x protocol. It provides a port for the client to access the LAN. The port can be a physical port or a logical port.
- The authentication server is used to implement user authentication, authorization, and accounting, and it is usually a RADIUS server.

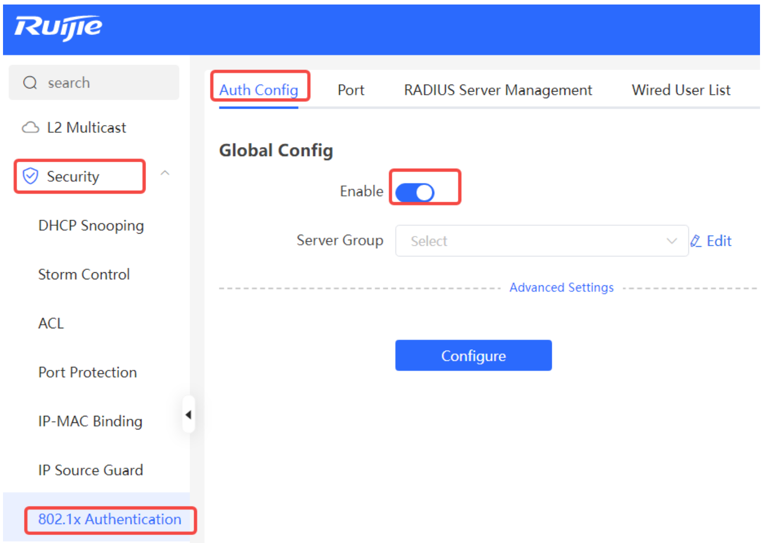
instruction

RG- NBS switching devices only support the authentication function.

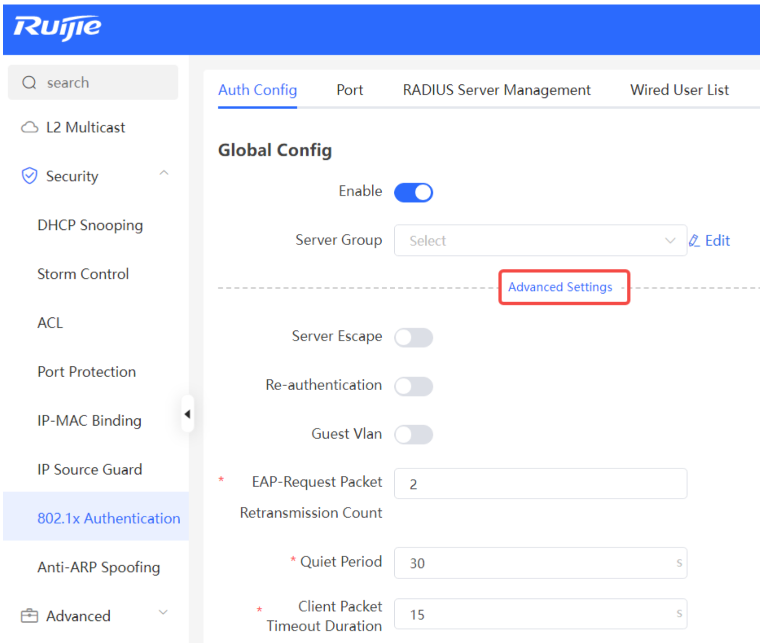
9.7.2 Configuration 802.1x

Choose **Local Device > Security** > **802.1x Authentication** > **Auth Config**

Toggle on **Global 802.1x**, the system prompts to confirm whether to enable it, click **Configure**.



Click Advanced Settings to configure parameters such as Guest VLAN.

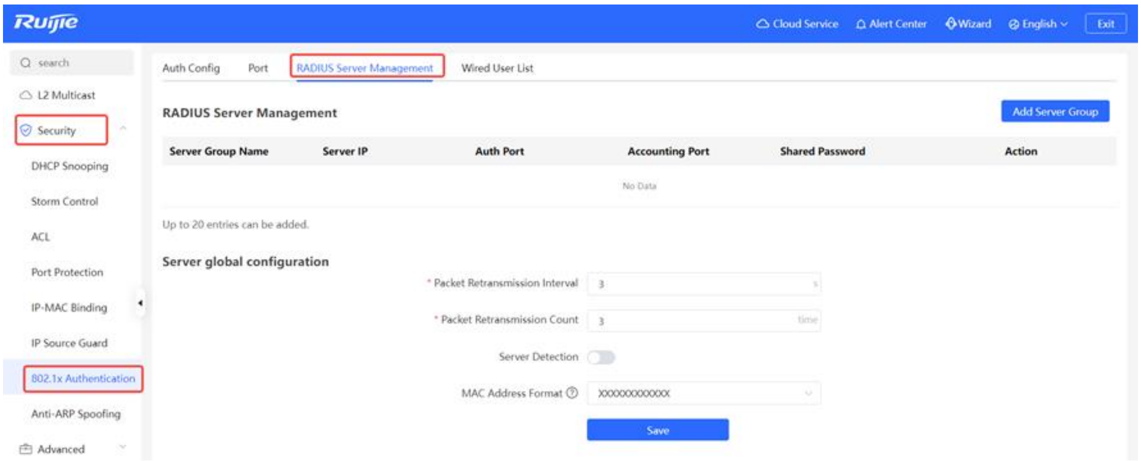


parameter	Description
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
EAP-Request Packet Retransmission Count	Define the number of times the EAP request message will be retransmitted when no response is received, value range: 1- 10 times
Quiet Period	During the authentication process, the idle time between the client and the server does not exchange authentication messages, value range: 0-65535 seconds
Client Packet Timeout Duration	The time limit for the server to wait for the response from the client. Exceeding this time will be regarded as an authentication failure. Value range: 1-65535 seconds
Client Packet Timeout Duration	The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication failure, value range: 1-65535 seconds
EAP-Request Packet Interval	Define the time interval between sending EAP request messages to control the rate of the authentication process, value range: 1-65535 seconds

(1) add server

Before configuration, please confirm:

- The Radius server is fully built and configured as follows.
  - Add username and password for client login.
  - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
  - A trusted IP on the Radius server.
- The network connection between the authentication device and the Radius server.
- IP addresses of the Radius server and the authentication device have been obtained.



RADIUS Server Management

Server Group Name	Server IP	Auth Port	Accounting Port	Shared Password	Action

No Data

Up to 20 entries can be added.

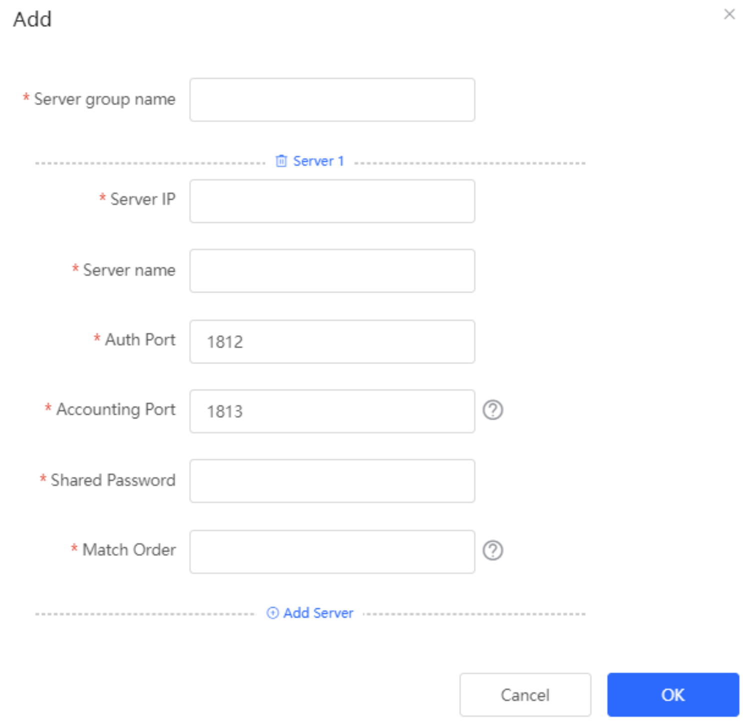
Server global configuration

* Packet Retransmission Interval: 3 s

* Packet Retransmission Count: 3 time

Server Detection

MAC Address Format: XXXXXXXXXXXX



* Server group name:

* Server IP:

* Server name:

* Auth Port: 1812

* Accounting Port: 1813

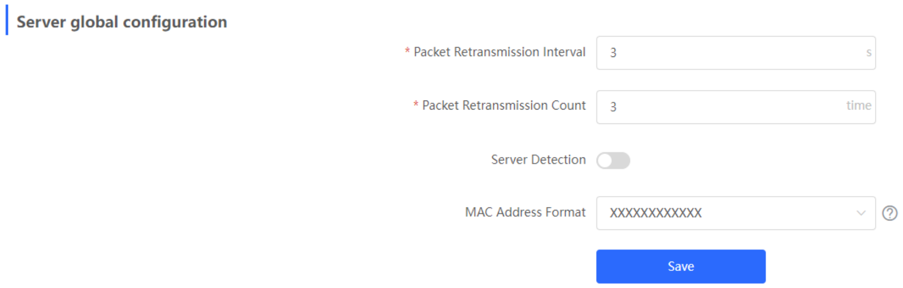
* Shared Password:

* Match Order:

parameter	Reference without translation	Description
Server group name		Server group name
Server IP	server address	Radius server address.
Auth Port	authentication port	The port number used for accessing user authentication on the Radius server.
Accounting Port	billing port	The port number used to access the accounting process on the Radius server.
Shared Password	shared password	Radius server shared key.
Match Order	matching order	The system supports adding up to 5 Radius servers.

parameter	Reference without translation	Description
		The higher the matching order value is, the higher the priority is.

(2) Set up the server and click **Save**.



Server global configuration

* Packet Retransmission Interval: 3 s

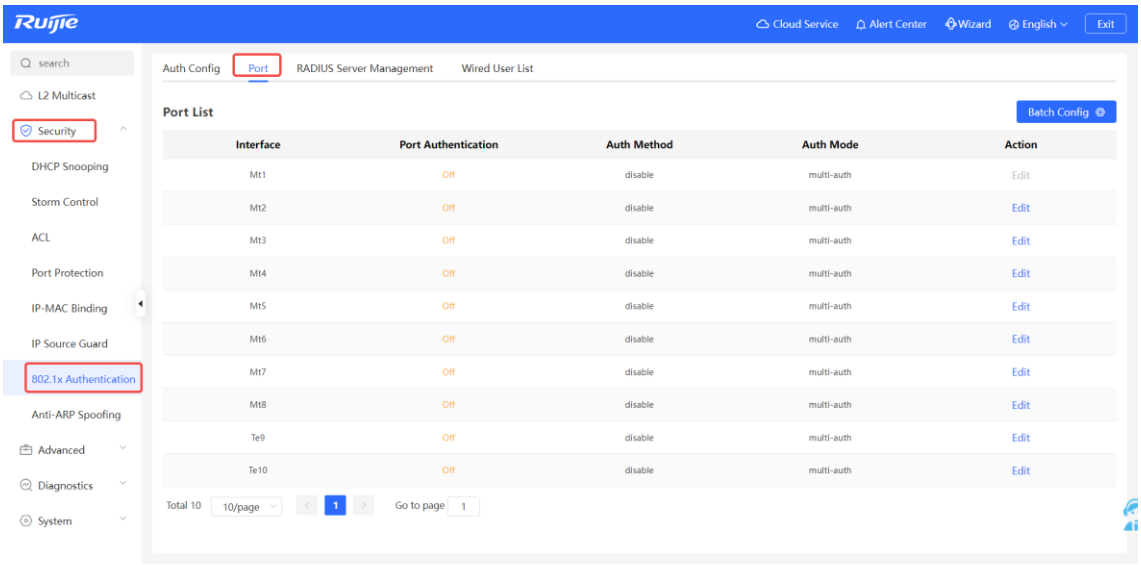
* Packet Retransmission Count: 3 time

Server Detection: ○

MAC Address Format: XXXXXXXXXXXX

Parameter	Description
Packet Retransmission Interval	Configure the interval for the device to send request packets before confirming that there is no response from RADIUS
Packet Retransmission Count	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
Server Detection	If this function is enabled, you need to set "Server Detection Period", "Server Detection Times" and "Server Detection Username". It is used to determine the status of the server, so as to decide whether to enable functions such as escape.
MAC Address Format	Configure the MAC address format of RADIUS attribute No. 31 (Calling-Stationg-ID). The following formats are supported: Dotted hexadecimal format, such as 00d0.f8aa.bbcc IETF format, such as 00-D0-F8-AA-BB-CC No format (default), e.g. 00d0f8aabbcc

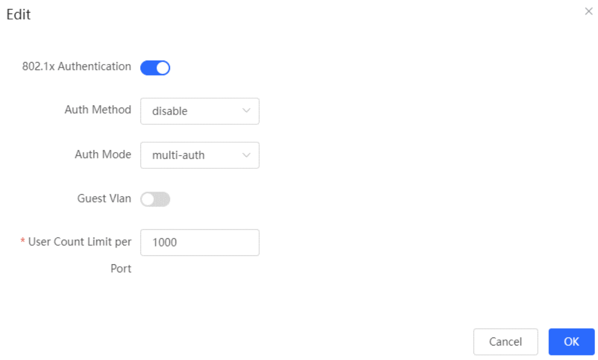
(3) Configure the effective interface, click interface configuration, click modify or batch configuration after a single interface, and edit the authentication parameters of the interface.



Port List

Interface	Port Authentication	Auth Method	Auth Mode	Action
Mt1	Off	disable	multi-auth	Edit
Mt2	Off	disable	multi-auth	Edit
Mt3	Off	disable	multi-auth	Edit
Mt4	Off	disable	multi-auth	Edit
Mt5	Off	disable	multi-auth	Edit
Mt6	Off	disable	multi-auth	Edit
Mt7	Off	disable	multi-auth	Edit
Mt8	Off	disable	multi-auth	Edit
Te9	Off	disable	multi-auth	Edit
Te10	Off	disable	multi-auth	Edit

Total 10 10/page 1 Go to page 1



Edit

802.1x Authentication: on

Auth Method: disable

Auth Mode: multi-auth

Guest Vlan: off

* User Count Limit per Port: 1000

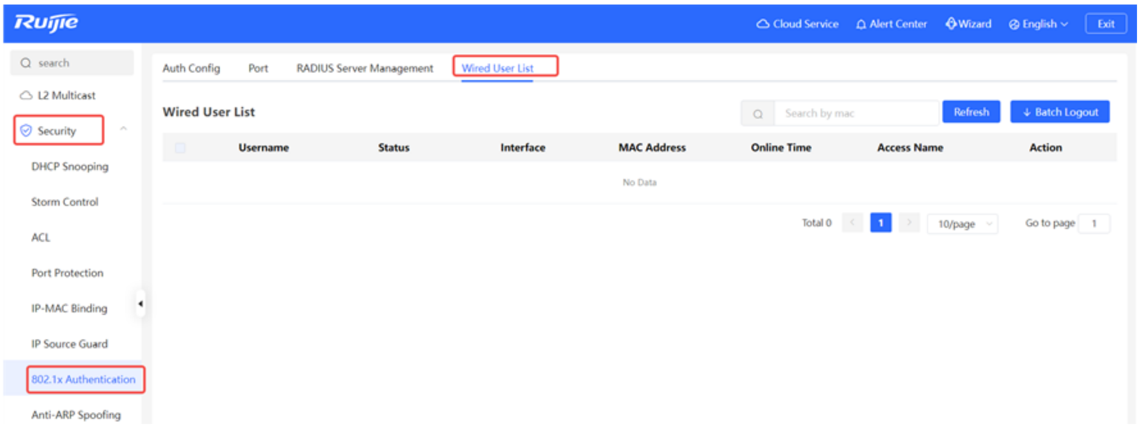
parameter	Description
802.1x Authentication	When enabled, the selected interface will enable 8.02.1x authentication.
Auth Method	disable: Turn off the authentication method, which has the same effect as turning off the 802.1x authentication switch force-auth: Mandatory authentication, the client can directly access the Internet without a password force-unauth: force no authentication, the client cannot authenticate and cannot access the Internet auto: automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication It is recommended to select the auto authentication method.
Auth Mode	multi-auth: Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently multi-host: Multiple devices are allowed to share the same port. As long as one user passes the authentication, subsequent users can access the

parameter	Description
	Internet single-host: Each port only allows one device to be authenticated, and can access the Internet after successful authentication
Guest Vlan	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN Note You need to create a VLAN ID first and apply it to the interface, then in Security Management > 802.1x Authentication > Advanced settings in the authentication configuration enable Guest VLAN and enter the ID
User Count Limit per Port	Limit the number of users under the interface Product Difference Description

9.7.3 View the list of wired authentication users

802.1x function is configured on the entire network and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

Choose **Local Device** > **Security Management > 802.1x Authentication** to obtain specific user information.



Wired User List

□	Username	Status	Interface	MAC Address	Online Time	Access Name	Action
No Data							

Click **Refresh** to get the latest user list information.

If you want to disconnect a certain user from the network, you can select the user and click **Offline** in the "Operation" column; you can also select multiple users and click **Batch Offline**.

9.8 Anti-ARP Spoofing

9.8.1 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.

9.8.2 Procedure

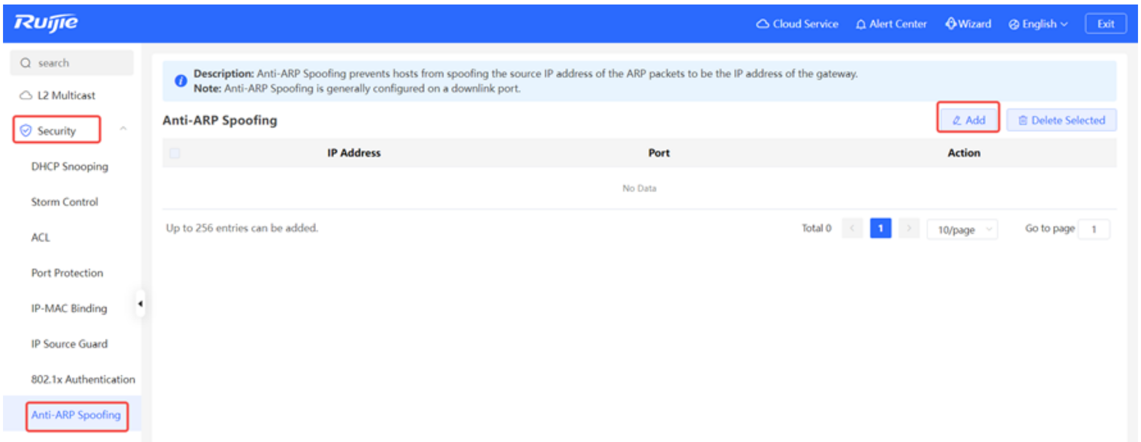
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

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.

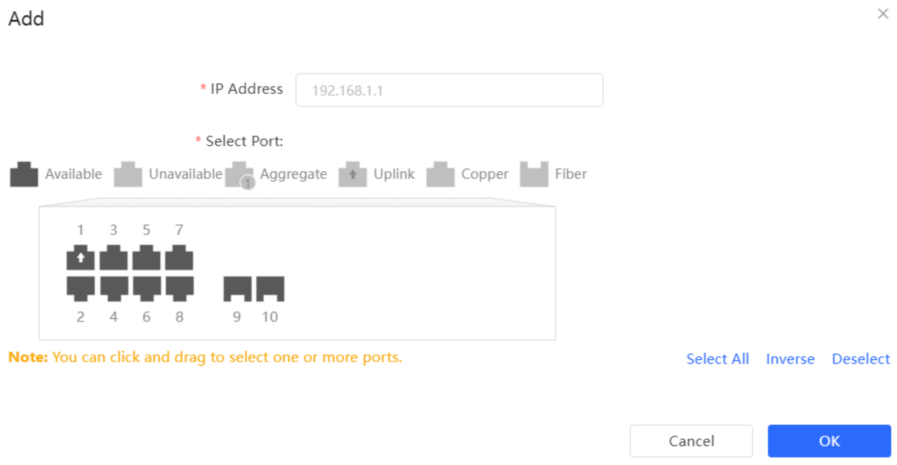


Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

IP Address	Port	Action
No Data		

Up to 256 entries can be added.



* IP Address: 192.168.1.1

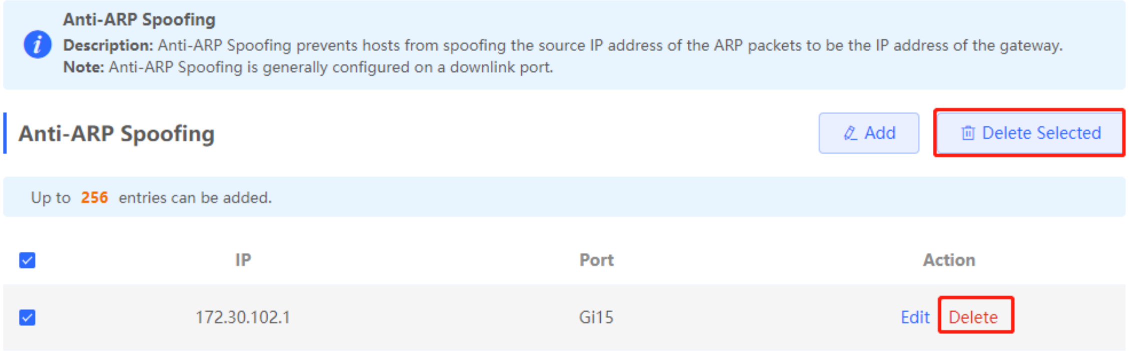
* Select Port:

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 **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.

Anti-ARP Spoofing

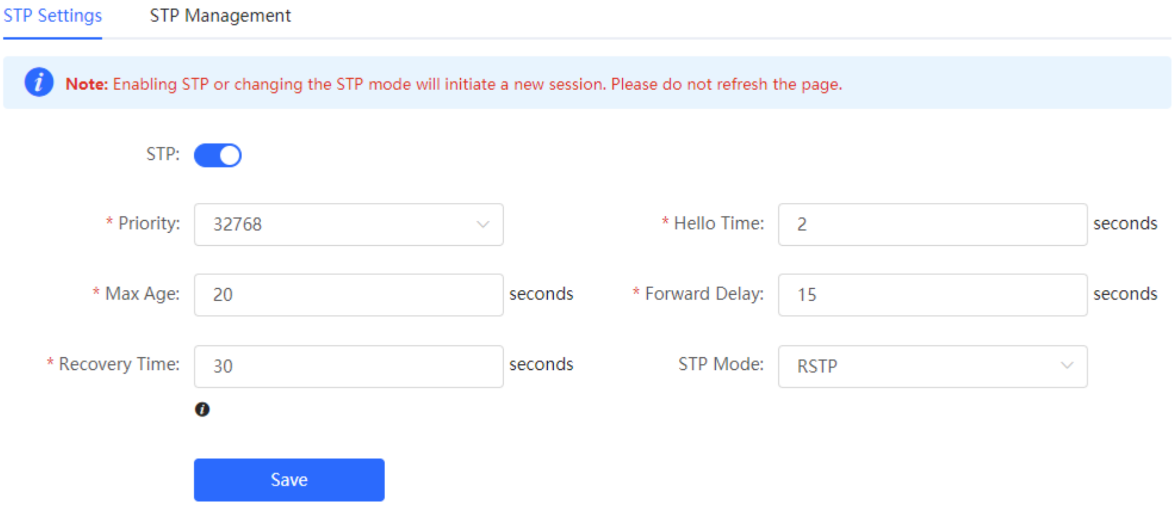
Up to 256 entries can be added.

☑	IP	Port	Action
☑	172.30.102.1	Gi15	Edit Delete

10 Advanced Configuration

10.1 STP

STP (Spanning Tree Protocol) is an L2 management protocol that eliminates L2 loops by selectively blocking redundant links on the network. It also provides the link backup function.



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

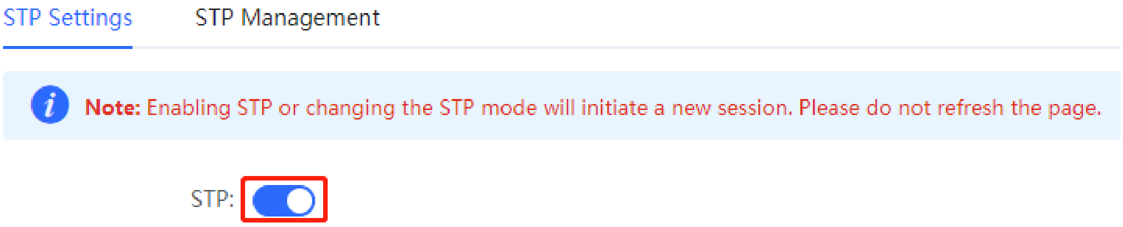
10.1.1 STP Global Settings

Choose **Local Device** > **Advanced** > **STP** > **STP**.

(1) Click to enable the STP function, and click OK in the displayed box. The STP function is disabled by default.

Caution

- After enabling the STP configuration of the device, the ERPS configuration cannot take effect normally.
- Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.

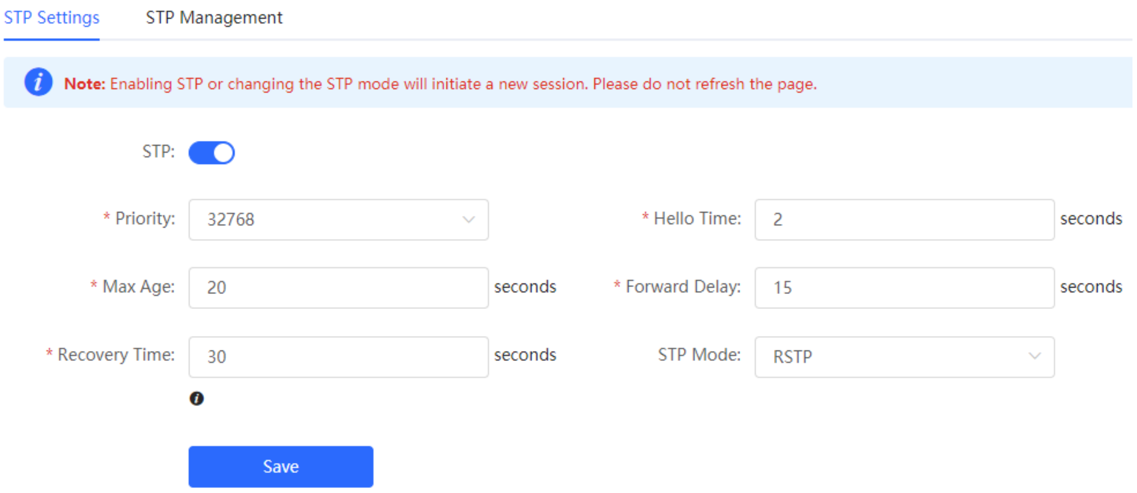


STP Settings | STP Management

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**.



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

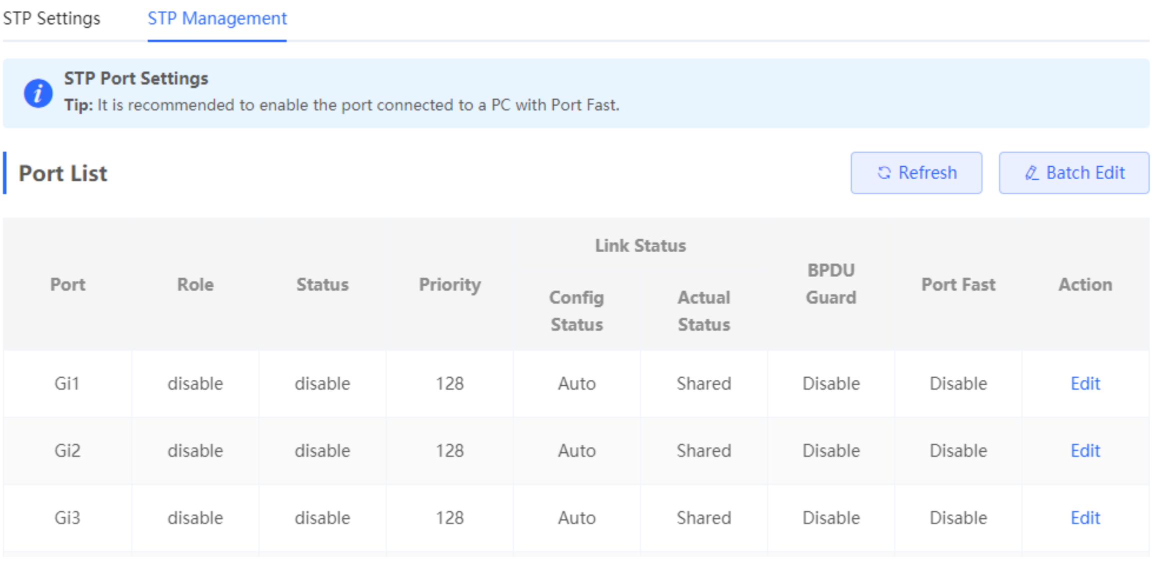
Table 10-1 Description of STP Global Configuration Parameters

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

10.1.2 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 the **Action** column in **Port List** to configure designated ports.

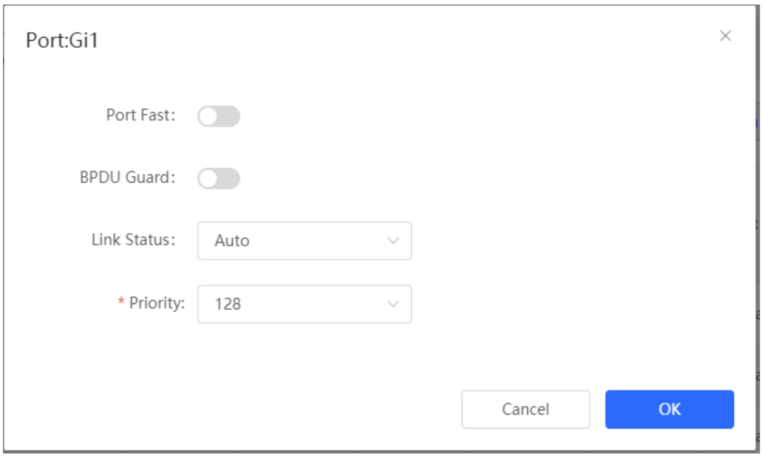


STP Port Settings

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 10-2 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 an upstream bridge to a downstream device. ● Disable (blocked ports): Ports that have no effect in the spanning tree.	N/A

Parameter	Description	Default Value
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.	N/A
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 Status	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	N/A
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
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.

10.2 LLDP

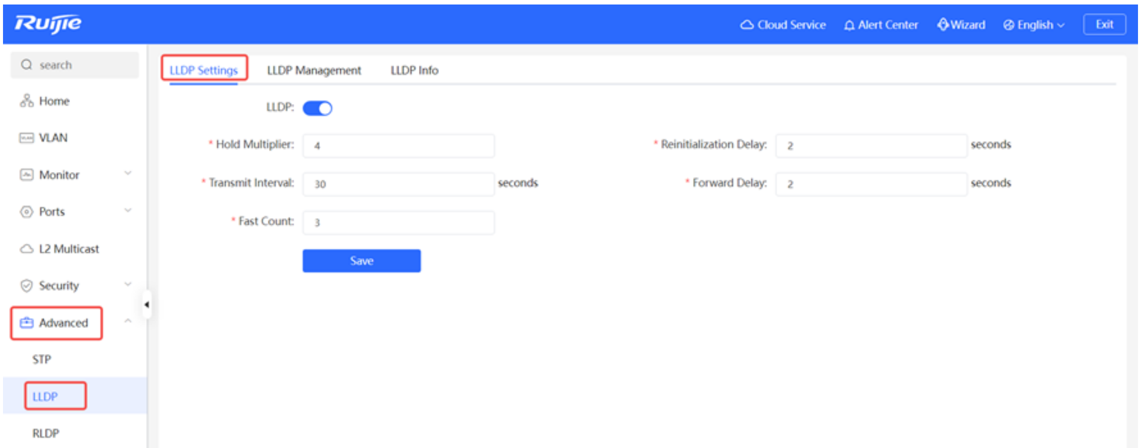
10.2.1 Overview

LLDP (Link Layer Discovery Protocol) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the web interface 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.

10.2.2 LLDP Global Settings

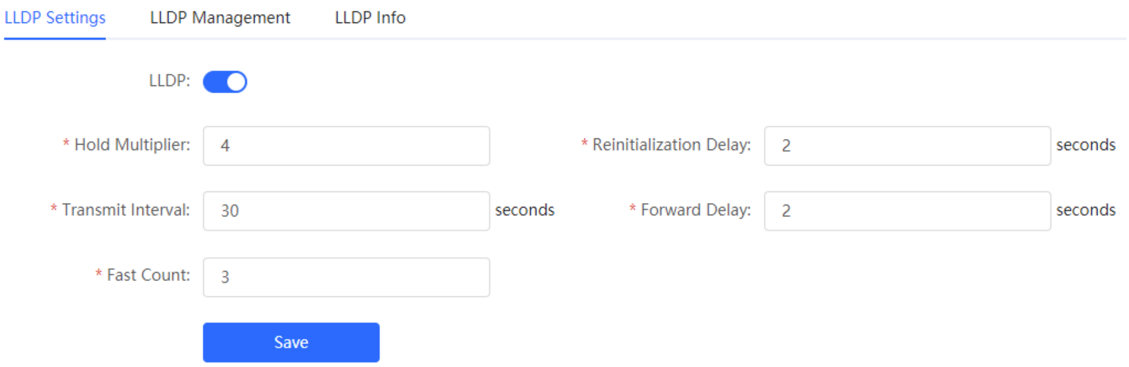
Choose **Local Device** > **Advanced** >**LLDP** > **LLDP Settings**.

(1) Click 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.



LLDP: ●
* Hold Multiplier: 4
* Reinitialization Delay: 2 seconds
* Transmit Interval: 30 seconds
* Forward Delay: 2 seconds
* Fast Count: 3

(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 10-3 Description of LLDP Global Configuration Parameters

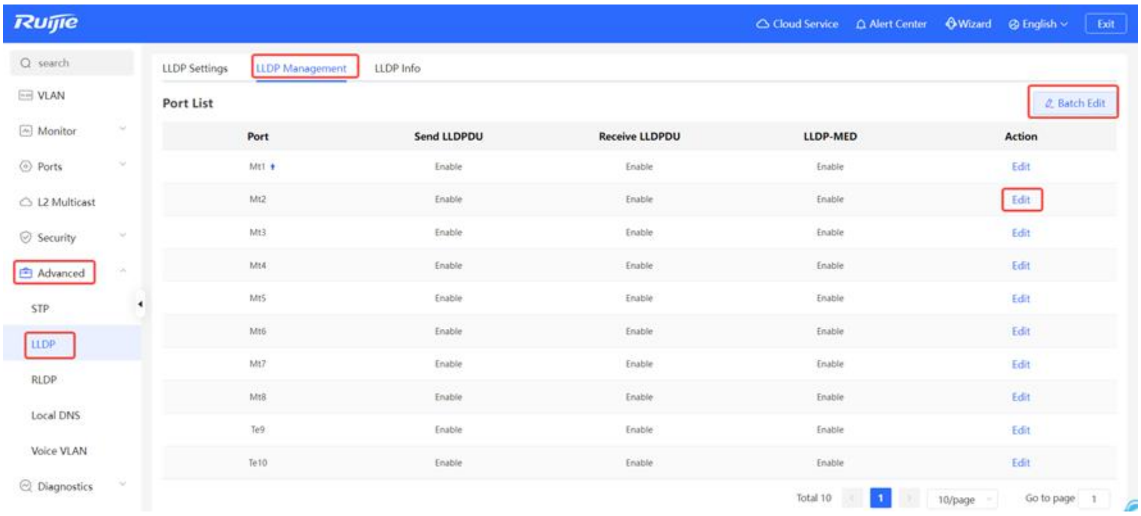
Parameter	Description	Default Value
LLDP	Indicates whether the LLDP function is enabled.	Enable
Hold Multiplier	TTL multiplier of LLDP In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor. The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier x 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 x 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
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

10.2.3 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**.

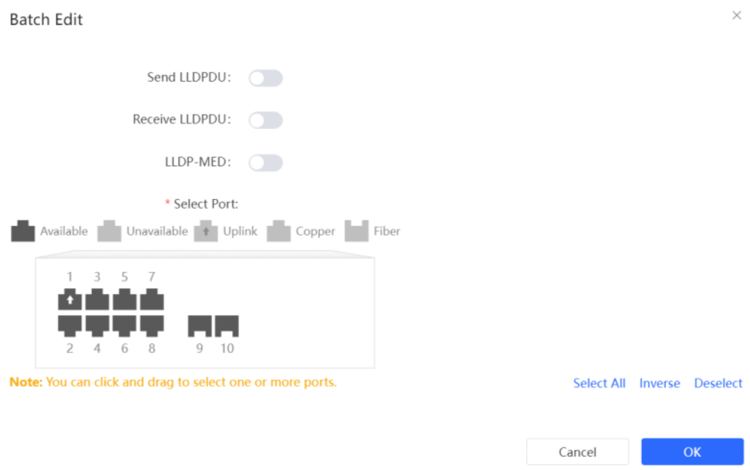
- **Send LLDPDU**: After **Send LLDPDU** is enabled on a port, the port can send LLDPDUs.
- **Receive LLDPDU**: After **Receive LLDPDU** is enabled on a port, the port can receive LLDPDUs.
- **LLDPMED**: After **LLDPMED** is enabled, the device is capable of discovering neighbors when its peer endpoint supports LLDP-MED (the Link Layer Discovery Protocol-Media Endpoint Discovery).



Port List

Port	Send LLDPDU	Receive LLDPDU	LLDP-MED	Action
Mt1	Enable	Enable	Enable	Edit
Mt2	Enable	Enable	Enable	Edit
Mt3	Enable	Enable	Enable	Edit
Mt4	Enable	Enable	Enable	Edit
Mt5	Enable	Enable	Enable	Edit
Mt6	Enable	Enable	Enable	Edit
Mt7	Enable	Enable	Enable	Edit
Mt8	Enable	Enable	Enable	Edit
Te9	Enable	Enable	Enable	Edit
Te10	Enable	Enable	Enable	Edit

Total 10 1 10/page Go to page 1


Batch Edit

Send LLDPDU: ○

Receive LLDPDU: ○

LLDP-MED: ○

* Select Port:

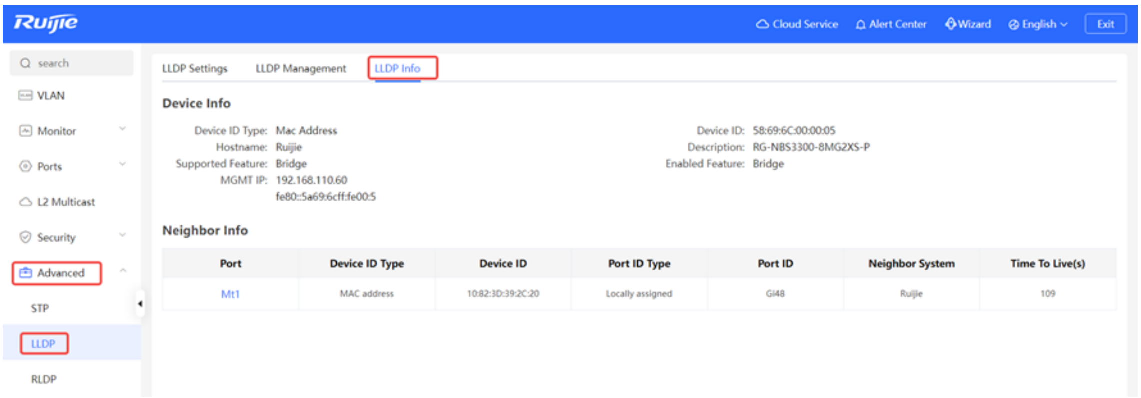
Note: You can click and drag to select one or more ports.

10.2.4 Displaying LLDP information

Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Info**.

To display LLDP information, 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 on 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.

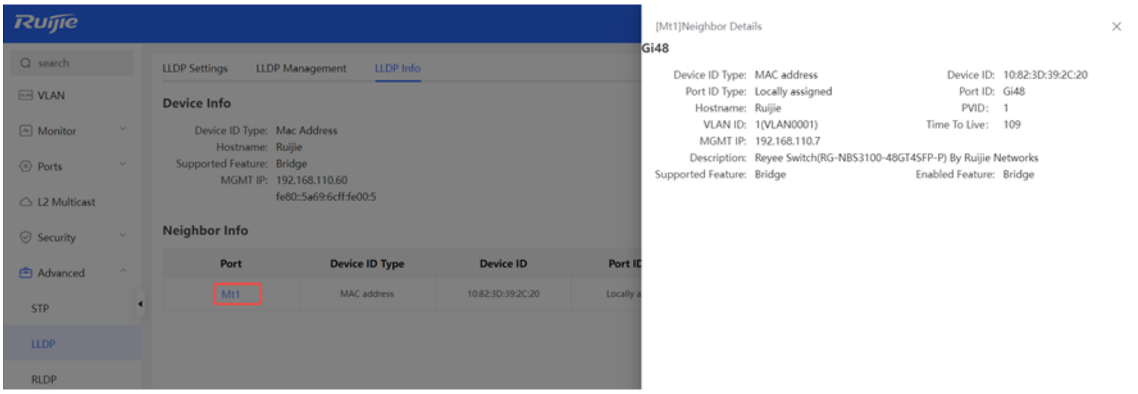


Device Info

Device ID Type: Mac Address
Hostname: Ruijie
Supported Feature: Bridge
MGMT IP: 192.168.110.60
fe80::5a69:6cff:fe00:5
Device ID: 58:69:6C:00:00:05
Description: RG-NBS3300-8MG2XS-P
Enabled Feature: Bridge

Neighbor Info

Port	Device ID Type	Device ID	Port ID Type	Port ID	Neighbor System	Time To Live(s)
Mt1	MAC address	10:82:3D:39:2C:20	Locally assigned	Gi48	Ruijie	109



[Mt1]Neighbor Details

Gi48

Device ID Type: MAC address
Port ID Type: Locally assigned
Hostname: Ruijie
VLAN ID: 1(VLAN0001)
MGMT IP: 192.168.110.7
Description: Reyee Switch(RG-NBS3100-48GT4SFP-P) By Ruijie Networks
Supported Feature: Bridge
Device ID: 10:82:3D:39:2C:20
Port ID: Gi48
PVID: 1
Time To Live: 109
Enabled Feature: Bridge

10.3 RLDP

10.3.1 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.

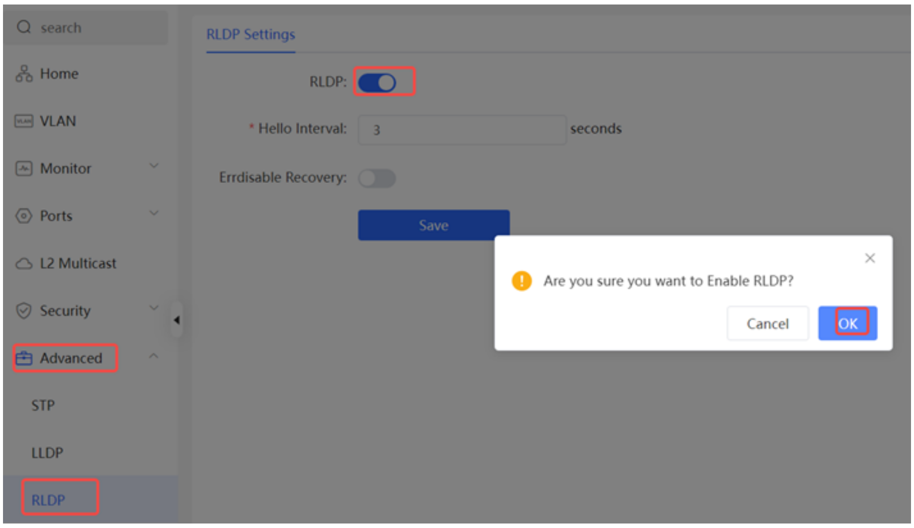
Supports enabling the RLDP function of the access switches on the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and the handling methods after a link fault is detected.

10.3.2 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.



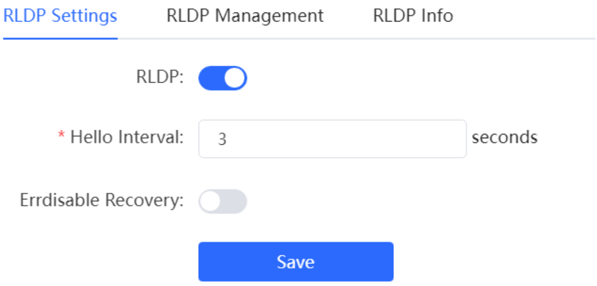
RLDP: ●

* Hello Interval: 3 seconds

Errdisable Recovery: ○

Are you sure you want to Enable RLDP?

(2) Configure RLDP global parameters and click **Save**.



RLDP: ●

* Hello Interval: 3 seconds

Errdisable Recovery: ○

Table 10-4 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**.

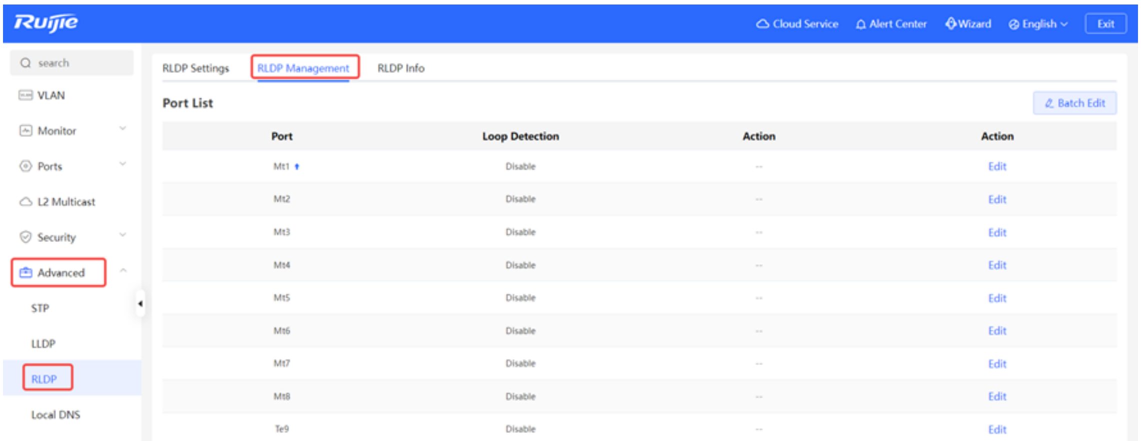
There are three methods to handle port failures:

- 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.

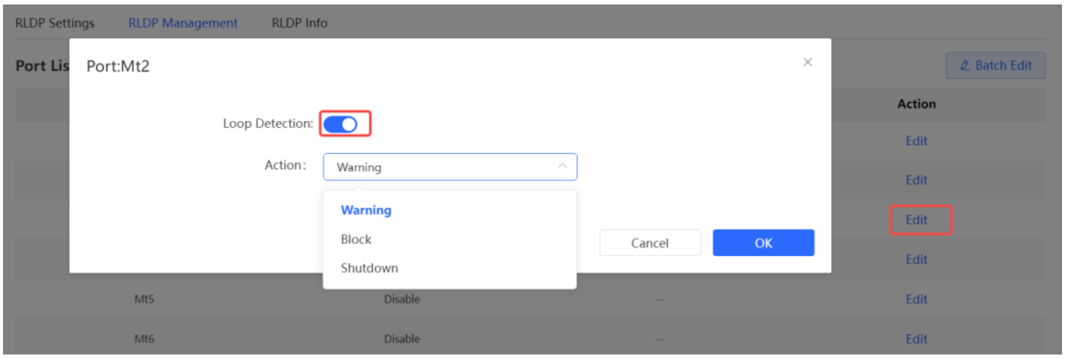
Caution

- 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
Mt1	Disable	--	Edit
Mt2	Disable	--	Edit
Mt3	Disable	--	Edit
Mt4	Disable	--	Edit
Mt5	Disable	--	Edit
Mt6	Disable	--	Edit
Mt7	Disable	--	Edit
Mt8	Disable	--	Edit
Te9	Disable	--	Edit



Port:Mt2

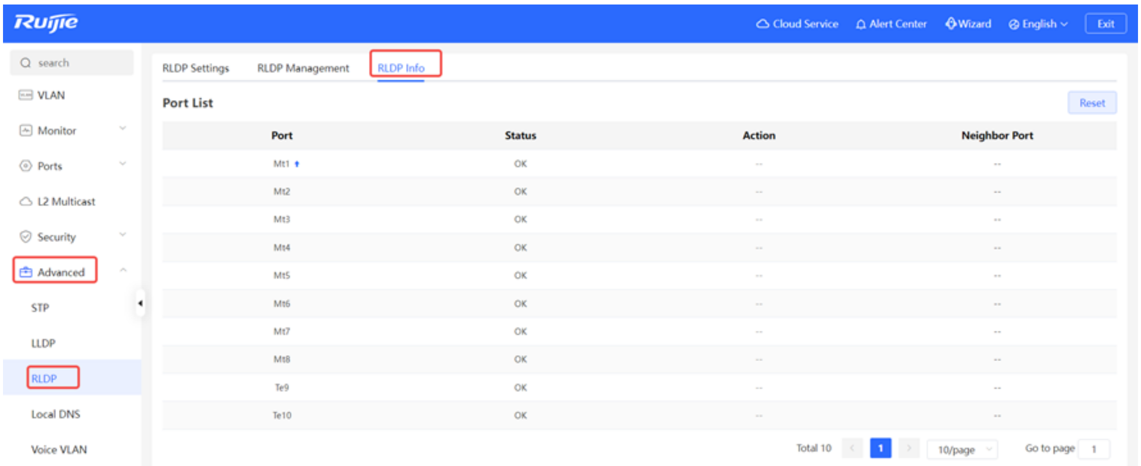
Loop Detection: ●

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.



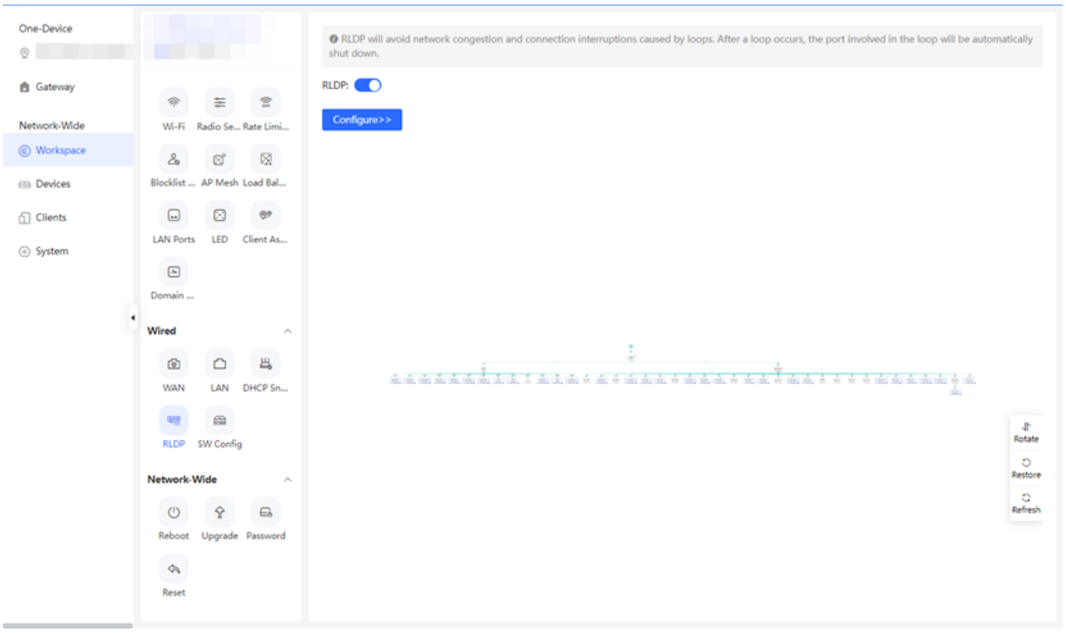
Port List

Port	Status	Action	Neighbor Port
Mt1	OK	--	--
Mt2	OK	--	--
Mt3	OK	--	--
Mt4	OK	--	--
Mt5	OK	--	--
Mt6	OK	--	--
Mt7	OK	--	--
Mt8	OK	--	--
Te9	OK	--	--
Te10	OK	--	--

10.3.3 Batch Configuring Network Switches

Choose **Network-Wide** > **Workspace** > **Wired** > **RLDP**

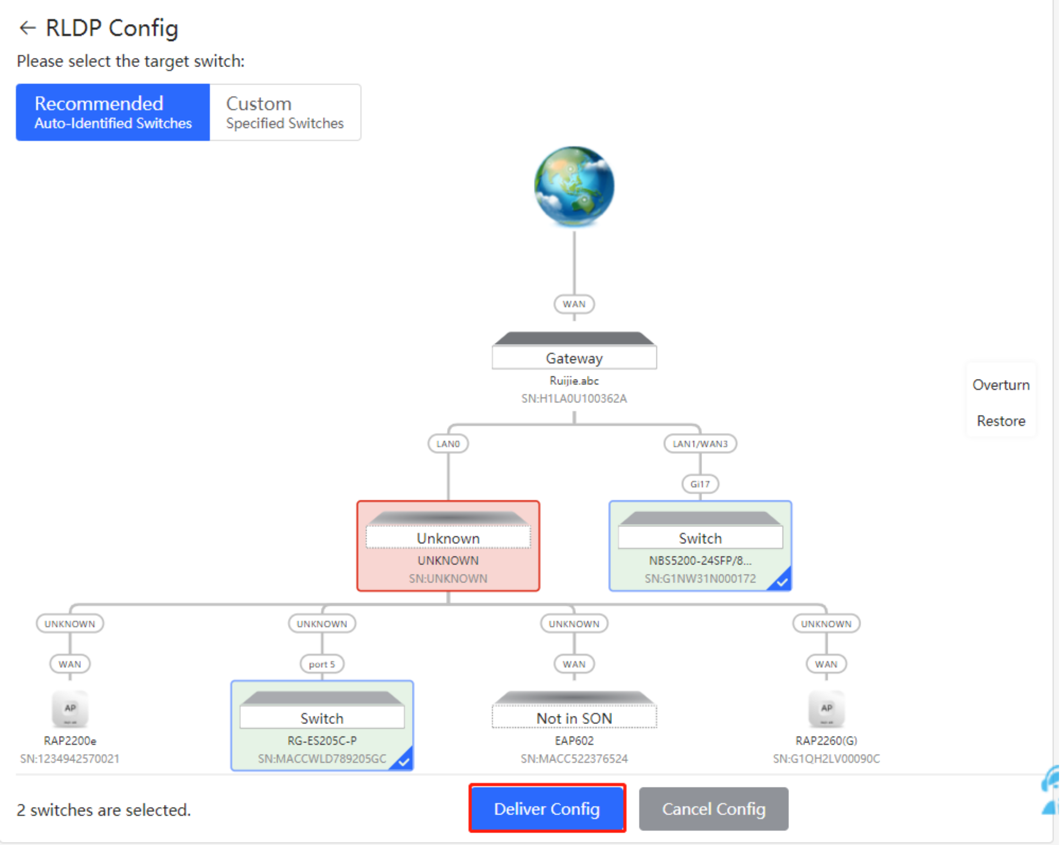
(1) Click **Enable** to access the **RLDP Config** page.



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: ●

(2) On 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 on 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.

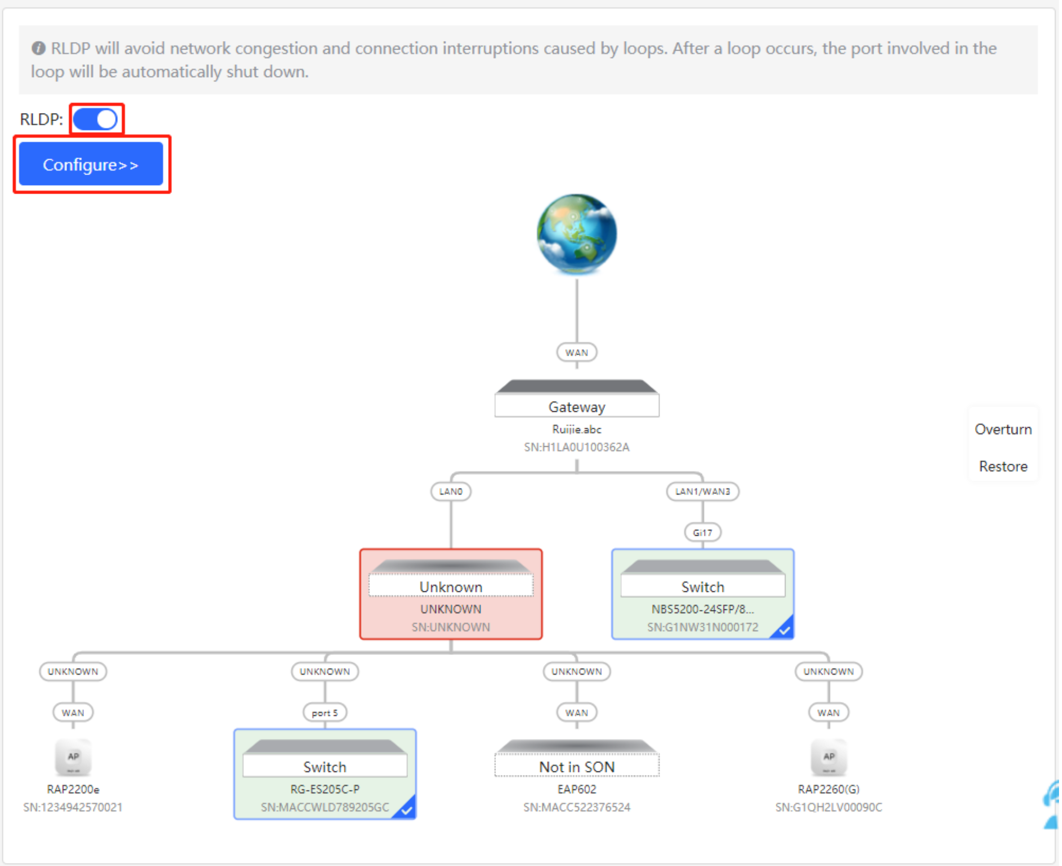


← RLDP Config

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.

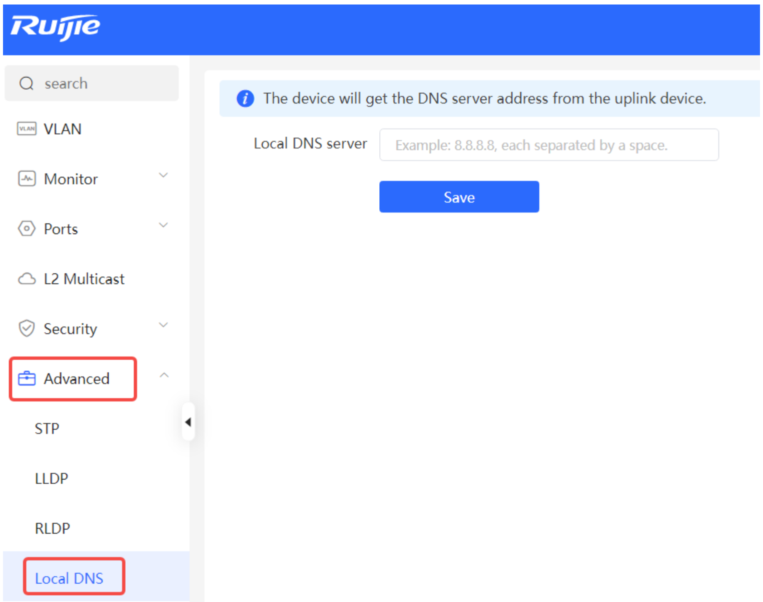
RLDP: ●

10.4 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.

10.5 Voice VLAN

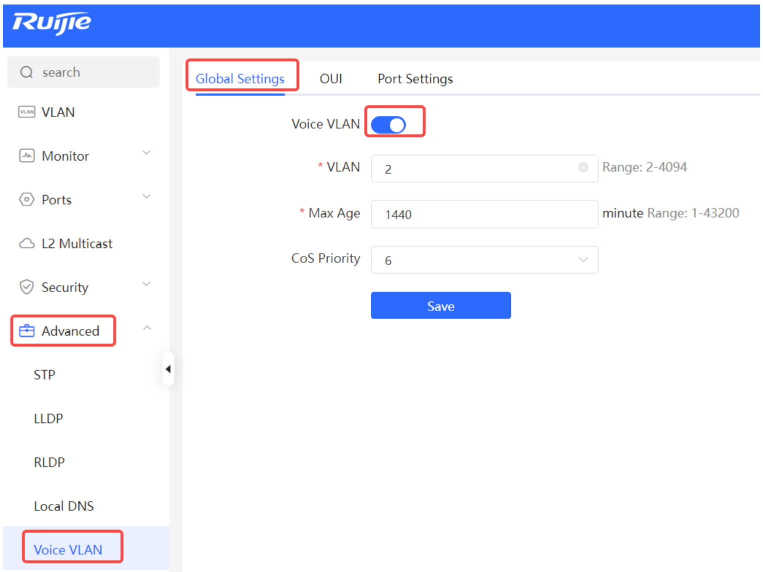
10.5.1 Overview

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.

10.5.2 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 10-5 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	N/A
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

10.5.3 Configuring a Voice VLAN OUI

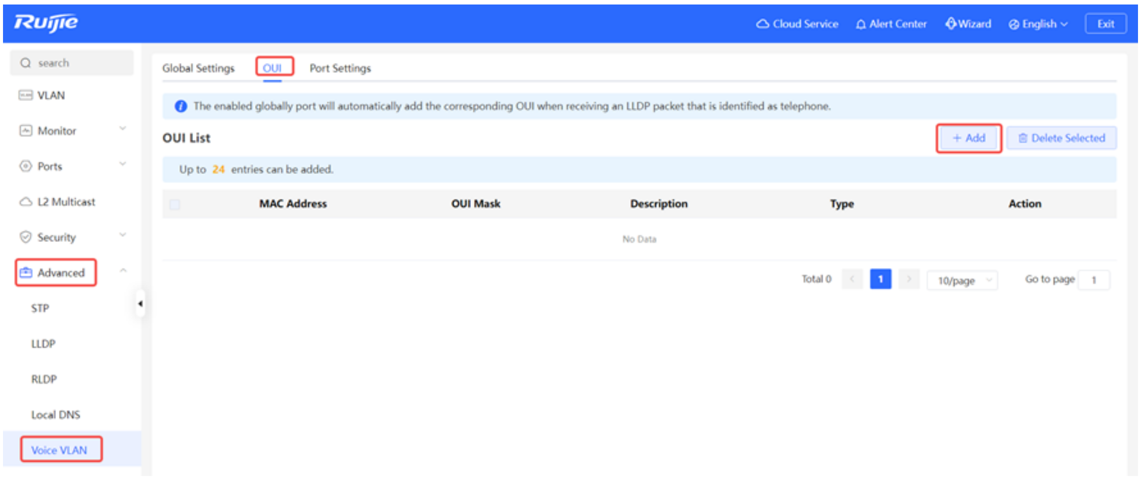
Choose **Local Device** > **Advanced** > **Voice VLAN** > **OUI**.

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 also 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**.



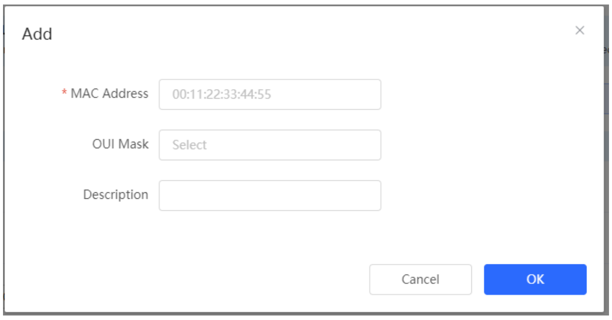
The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

OUI List

Up to 24 entries can be added.

MAC Address	OUI Mask	Description	Type	Action

No Data

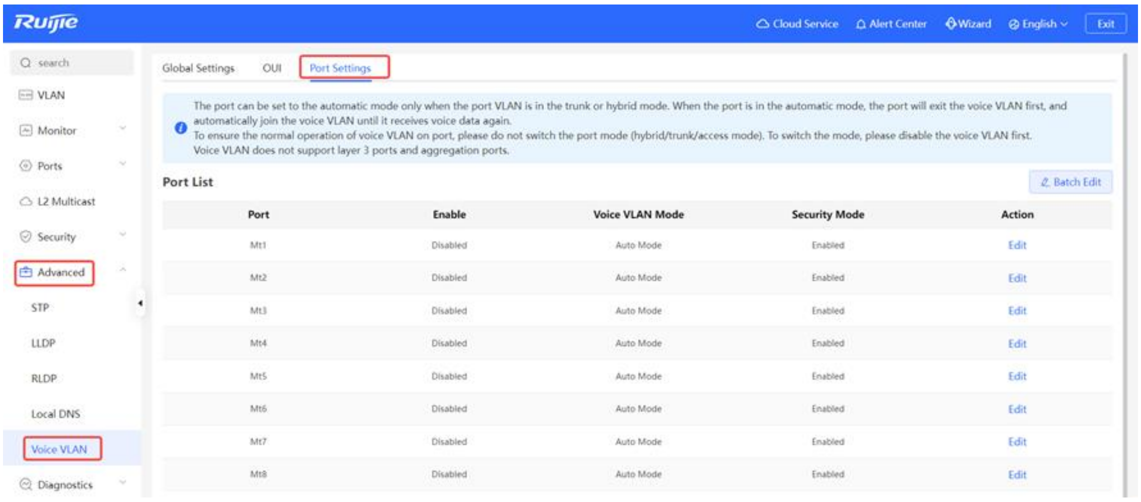


* MAC Address	00:11:22:33:44:55
OUI Mask	Select
Description	

10.5.4 Configuring the Voice VLAN Function on a Port

Choose **Local Device** > **Advanced** > **Voice VLAN** > **Port Settings**.

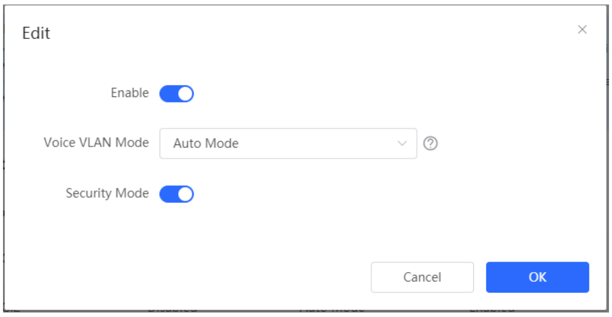
Click **Edit** in the port entry or click **Batch Edit** on the upper -right corner. In the displayed dialog box, select whether to enable the voice VLAN function on the port, voice VLAN mode to be applied, and whether to enable the security mode, and Click **OK**.



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
Mt1	Disabled	Auto Mode	Enabled	Edit
Mt2	Disabled	Auto Mode	Enabled	Edit
Mt3	Disabled	Auto Mode	Enabled	Edit
Mt4	Disabled	Auto Mode	Enabled	Edit
Mt5	Disabled	Auto Mode	Enabled	Edit
Mt6	Disabled	Auto Mode	Enabled	Edit
Mt7	Disabled	Auto Mode	Enabled	Edit
Mt8	Disabled	Auto Mode	Enabled	Edit



Enable	●
Voice VLAN Mode	Auto Mode
Security Mode	●

Table 10-6 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

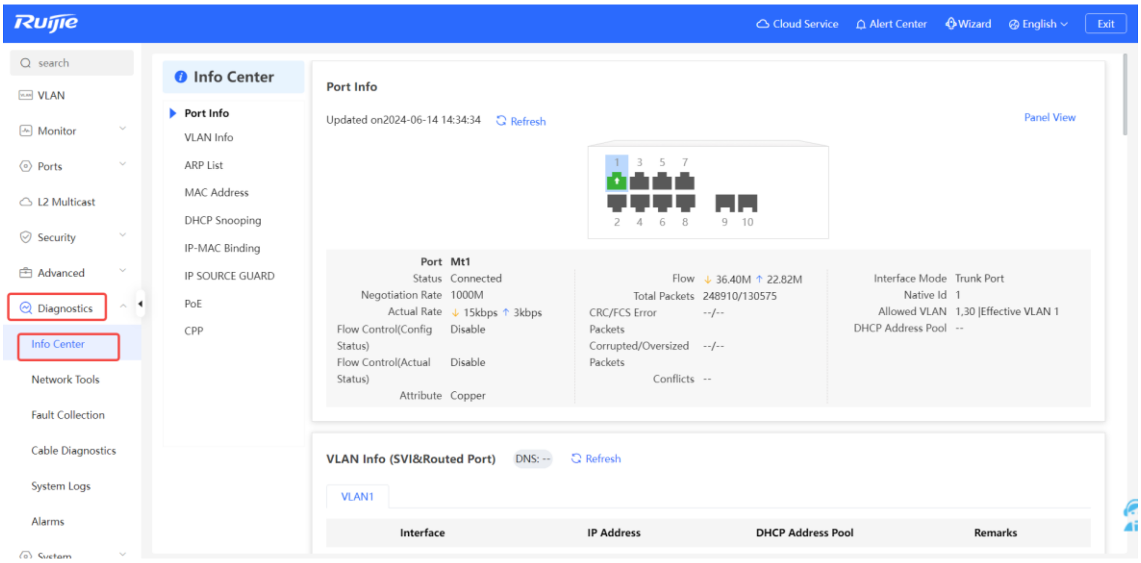
- The voice VLAN mode of the port can be set as the auto mode only when the VLAN mode of the port is Trunk mode. When the voice VLAN mode of the port work in the auto mode, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.
- After the voice 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.

11 Diagnostics

11.1 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 on2024-06-14 14:34:34

Port Mt1
Status Connected
Negotiation Rate 1000M
Actual Rate ↓ 15kbps ↑ 3kbps
Flow Control(Config Status) Disable
Flow Control(Actual Status) Disable
Attribute Copper

Flow ↓ 36.40M ↑ 22.82M
Total Packets 248910/130575
CRC/FCS Error Packets --/--
Corrupted/Oversized Packets --/--
Conflicts --

Interface Mode Trunk Port
Native Id 1
Allowed VLAN 1,30 |Effective VLAN 1
DHCP Address Pool --

VLAN Info (SVI&Routed Port) DNS: --

Interface	IP Address	DHCP Address Pool	Remarks

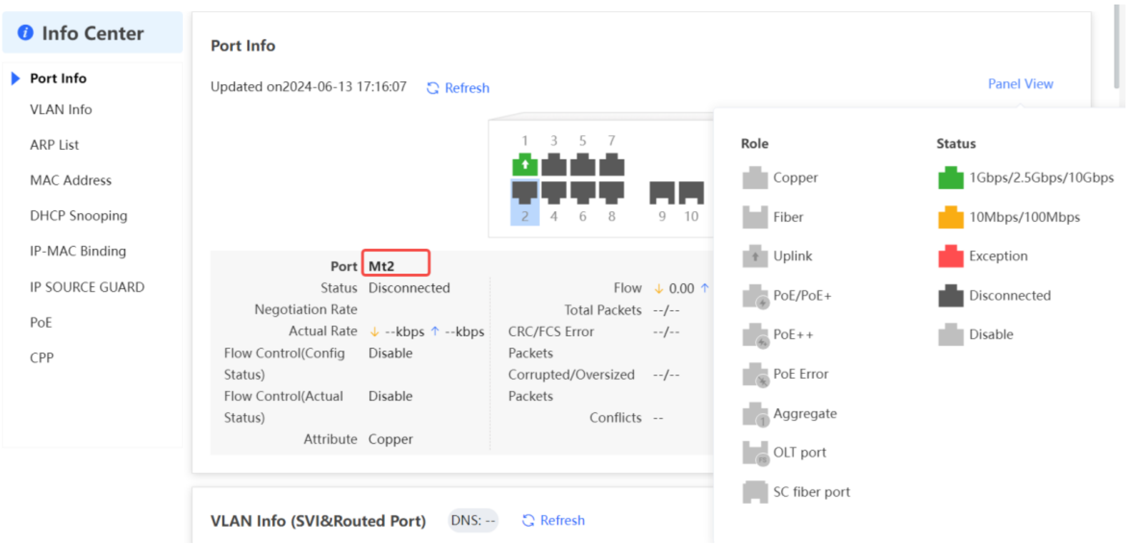
11.1.1 Port Info

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 7.2 Port Configuration.
- To configure the L2 mode of the port and the VLAN to which it belongs, see 5.3 Configuring Port VLAN.



Port Info

Updated on2024-06-13 17:16:07 Refresh

Panel View

Port Mt2
Status Disconnected
Negotiation Rate
Actual Rate ↓ --kbps ↑ --kbps
Flow Control(Config Status) Disable
Flow Control(Actual Status) Disable
Attribute Copper

Flow ↓ 0.00 ↑
Total Packets --/--
CRC/FCS Error Packets --/--
Corrupted/Oversized Packets --/--
Conflicts --

Role	Status
Copper	🟩 1Gbps/2.5Gbps/10Gbps
Fiber	🟧 10Mbps/100Mbps
Uplink	🟥 Exception
PoE/PoE+	⬛ Disconnected
PoE++	⬜ Disable
PoE Error	
Aggregate	
OLT port	
SC fiber port	

VLAN Info (SVI&Routed Port) DNS: -- Refresh

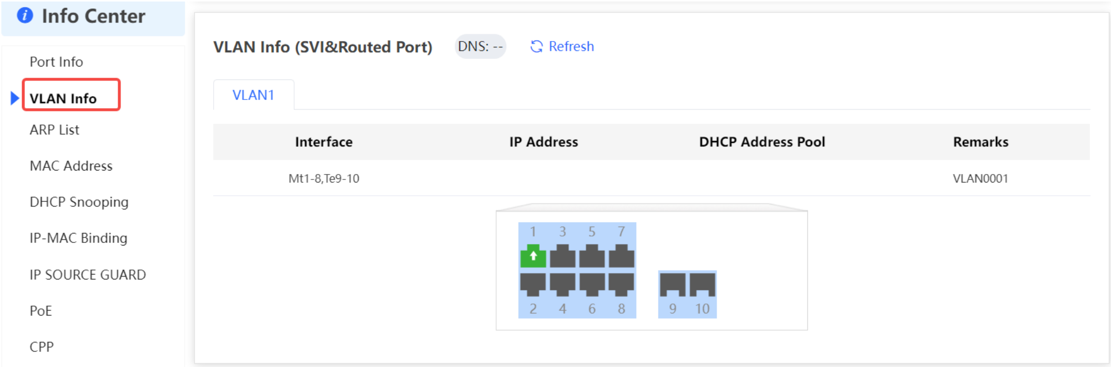
11.1.2 VLAN Info

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 5 VLAN.



VLAN Info (SVI&Routed Port) DNS: -- Refresh

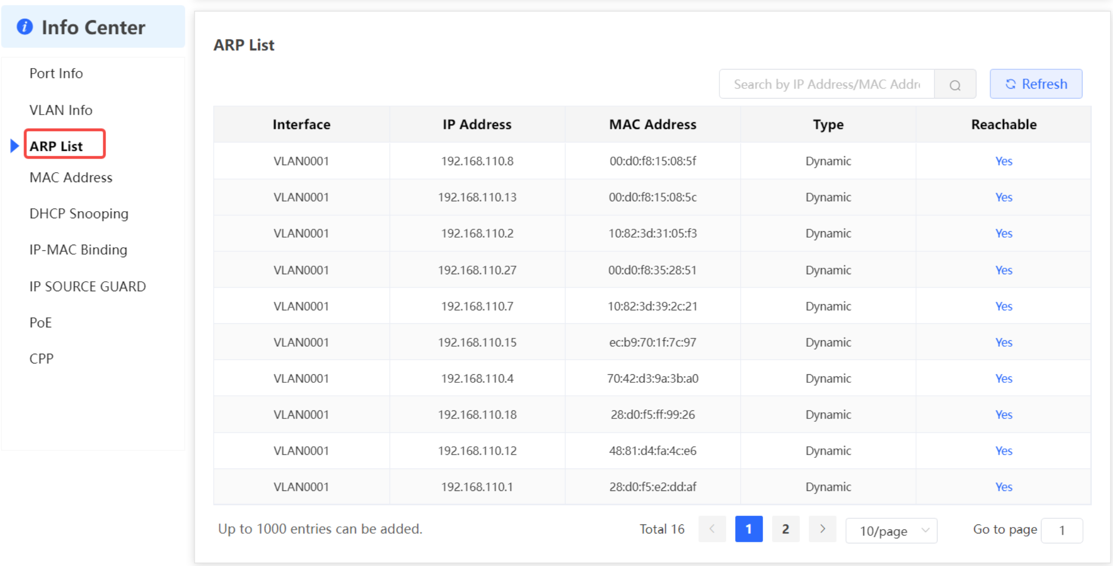
VLAN1

Interface	IP Address	DHCP Address Pool	Remarks
Mt1-8,Te9-10			VLAN0001

11.1.3 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.



ARP List

Interface	IP Address	MAC Address	Type	Reachable
VLAN0001	192.168.110.8	00:d0:f8:15:08:5f	Dynamic	Yes
VLAN0001	192.168.110.13	00:d0:f8:15:08:5c	Dynamic	Yes
VLAN0001	192.168.110.2	10:82:3d:31:05:f3	Dynamic	Yes
VLAN0001	192.168.110.27	00:d0:f8:35:28:51	Dynamic	Yes
VLAN0001	192.168.110.7	10:82:3d:39:2c:21	Dynamic	Yes
VLAN0001	192.168.110.15	ec:b9:70:1f:7c:97	Dynamic	Yes
VLAN0001	192.168.110.4	70:42:d3:9a:3b:a0	Dynamic	Yes
VLAN0001	192.168.110.18	28:d0:f5:ff:99:26	Dynamic	Yes
VLAN0001	192.168.110.12	48:81:d4:fa:4c:e6	Dynamic	Yes
VLAN0001	192.168.110.1	28:d0:f5:e2:dd:af	Dynamic	Yes

Up to 1000 entries can be added.

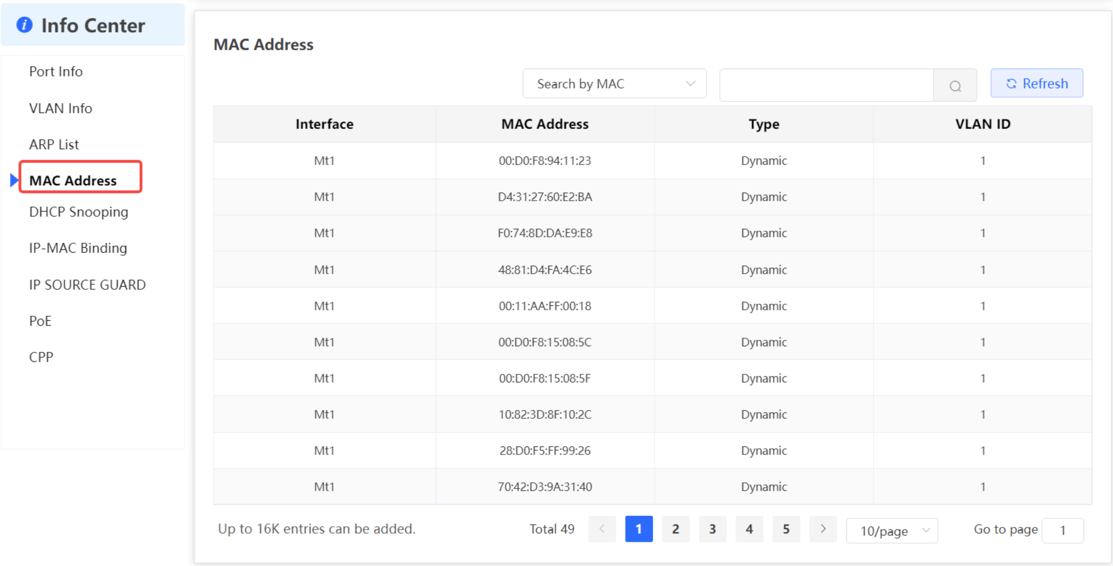
11.1.4 MAC Address

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 6.2 Client Management.



MAC Address

Interface	MAC Address	Type	VLAN ID
Mt1	00:D0:F8:94:11:23	Dynamic	1
Mt1	D4:31:27:60:E2:BA	Dynamic	1
Mt1	F0:74:8D:DA:E9:E8	Dynamic	1
Mt1	48:81:D4:FA:4C:E6	Dynamic	1
Mt1	00:11:AA:FF:00:18	Dynamic	1
Mt1	00:D0:F8:15:08:5C	Dynamic	1
Mt1	00:D0:F8:15:08:5F	Dynamic	1
Mt1	10:82:3D:8F:10:2C	Dynamic	1
Mt1	28:D0:F5:FF:99:26	Dynamic	1
Mt1	70:42:D3:9A:31:40	Dynamic	1

Up to 16K entries can be added.

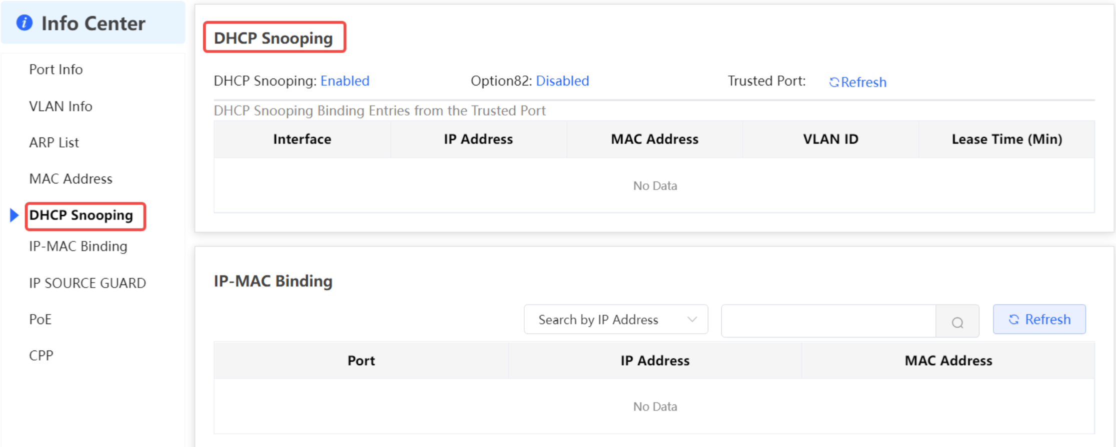
11.1.5 DHCP Snooping

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 9.1 DHCP Snooping.



DHCP Snooping

DHCP Snooping: Enabled Option82: Disabled Trusted Port:

DHCP Snooping Binding Entries from the Trusted Port

Interface	IP Address	MAC Address	VLAN ID	Lease Time (Min)
No Data				

IP-MAC Binding

Port	IP Address	MAC Address
No Data		

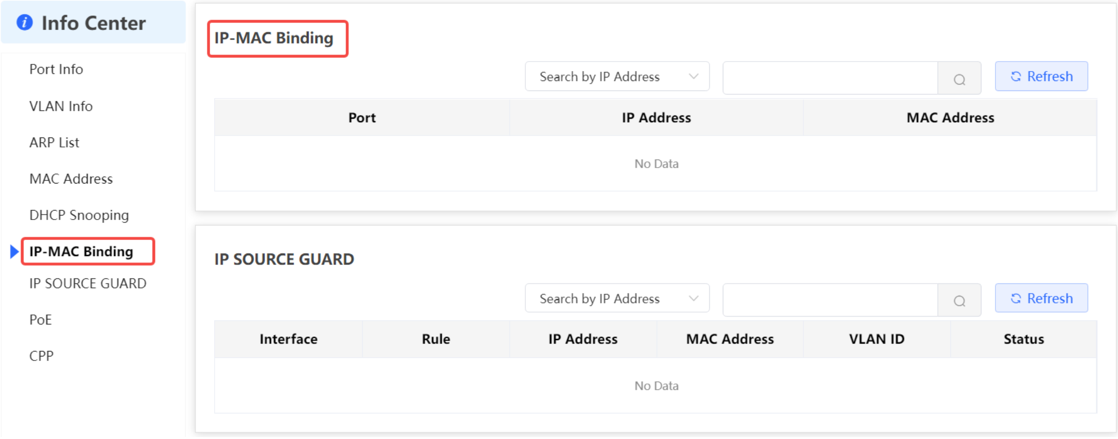
11.1.6 IP-MAC Binding

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 9.5 IP-MAC Binding.



IP-MAC Binding

Port	IP Address	MAC Address
No Data		

IP SOURCE GUARD

Interface	Rule	IP Address	MAC Address	VLAN ID	Status
No Data					

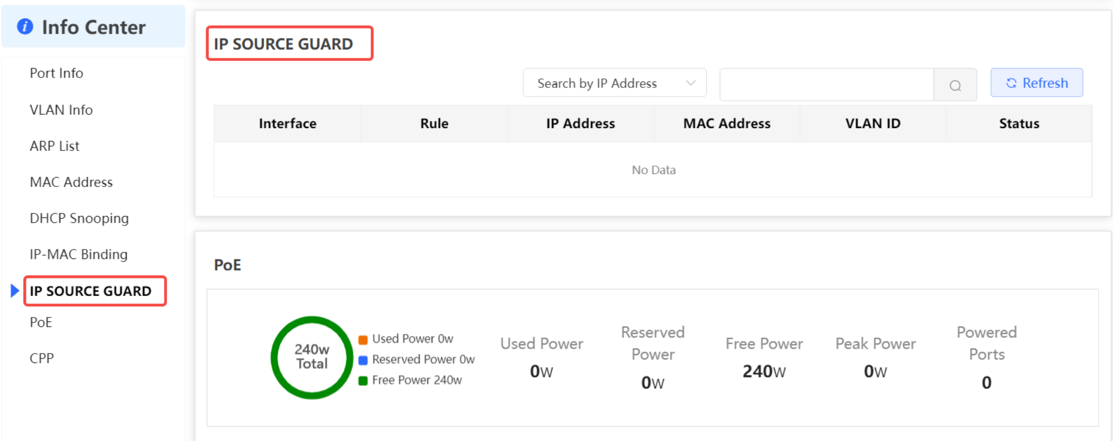
11.1.7 IP Source Guard

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 9.6 IP Source Guard.



IP SOURCE GUARD

Interface	Rule	IP Address	MAC Address	VLAN ID	Status

No Data

PoE

240w Total

- Used Power 0w
- Reserved Power 0w
- Free Power 240w

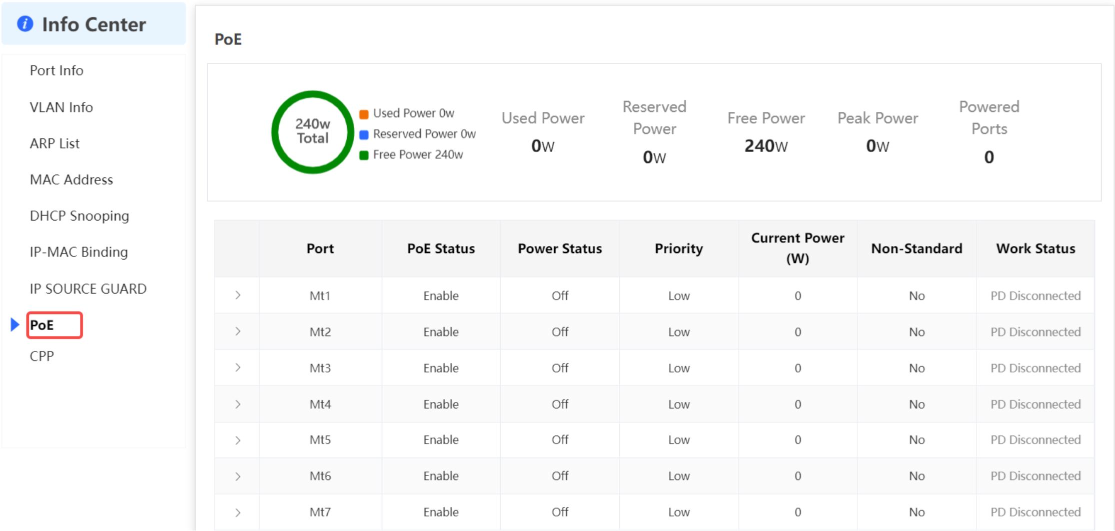
Used Power	Reserved Power	Free Power	Peak Power	Powered Ports
0w	0w	240w	0w	0

11.1.8 PoE

Caution

Only PoE switches (model name containing –P, -LP, -HP, and -UP) support this function.

Choose **Local Device** > **Diagnostics** > **Info Center** > **PoE.**



PoE

240w Total

- Used Power 0w
- Reserved Power 0w
- Free Power 240w

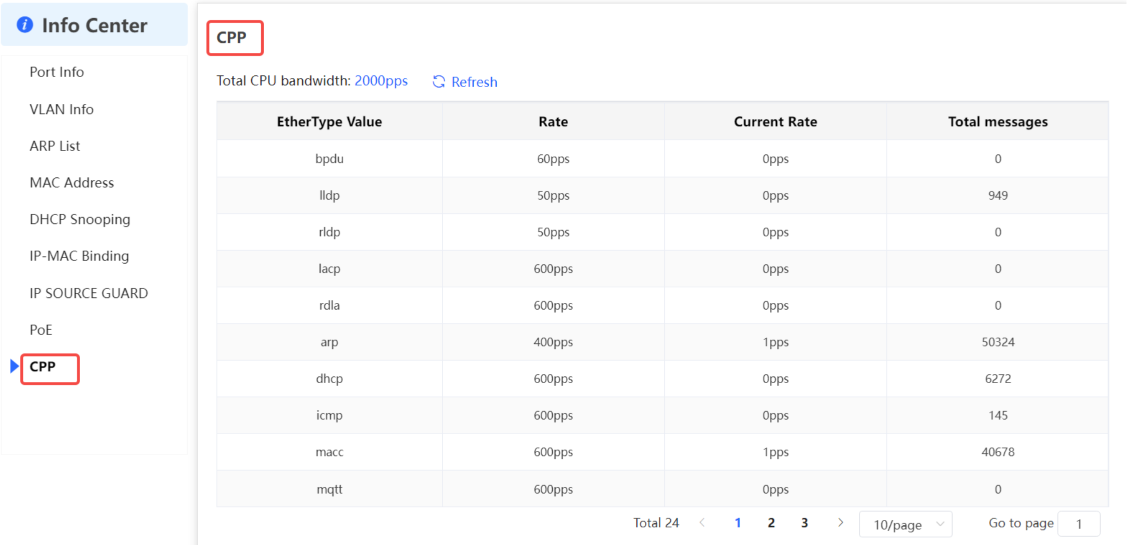
Used Power	Reserved Power	Free Power	Peak Power	Powered Ports
0w	0w	240w	0w	0

	Port	PoE Status	Power Status	Priority	Current Power (W)	Non-Standard	Work Status
>	Mt1	Enable	Off	Low	0	No	PD Disconnected
>	Mt2	Enable	Off	Low	0	No	PD Disconnected
>	Mt3	Enable	Off	Low	0	No	PD Disconnected
>	Mt4	Enable	Off	Low	0	No	PD Disconnected
>	Mt5	Enable	Off	Low	0	No	PD Disconnected
>	Mt6	Enable	Off	Low	0	No	PD Disconnected
>	Mt7	Enable	Off	Low	0	No	PD Disconnected

11.1.9 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 Refresh

EtherType Value	Rate	Current Rate	Total messages
bpdu	60pps	0pps	0
lldp	50pps	0pps	949
rldp	50pps	0pps	0
lacp	600pps	0pps	0
rdla	600pps	0pps	0
arp	400pps	1pps	50324
dhcp	600pps	0pps	6272
icmp	600pps	0pps	145
macc	600pps	1pps	40678
mqtt	600pps	0pps	0

Total 24 < 1 2 3 > 10/page Go to page 1

11.2 Network Tools

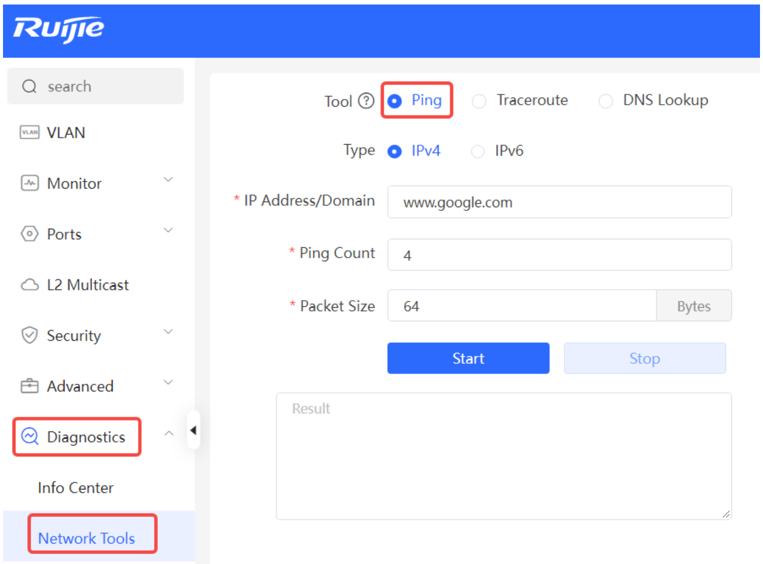
The **Network Tools** page provides three tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

11.2.1 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

Type ● IPv4 ○ IPv6

* IP Address/Domain www.google.com

* Ping Count 4

* Packet Size 64 Bytes

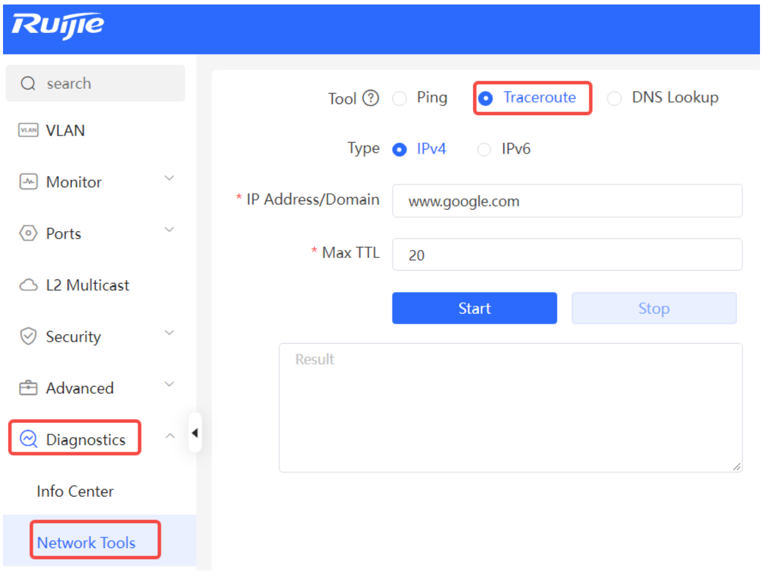
Result

11.2.2 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**.



Tool ○ Ping ● Traceroute ○ DNS Lookup

Type ● IPv4 ○ IPv6

* IP Address/Domain: www.google.com

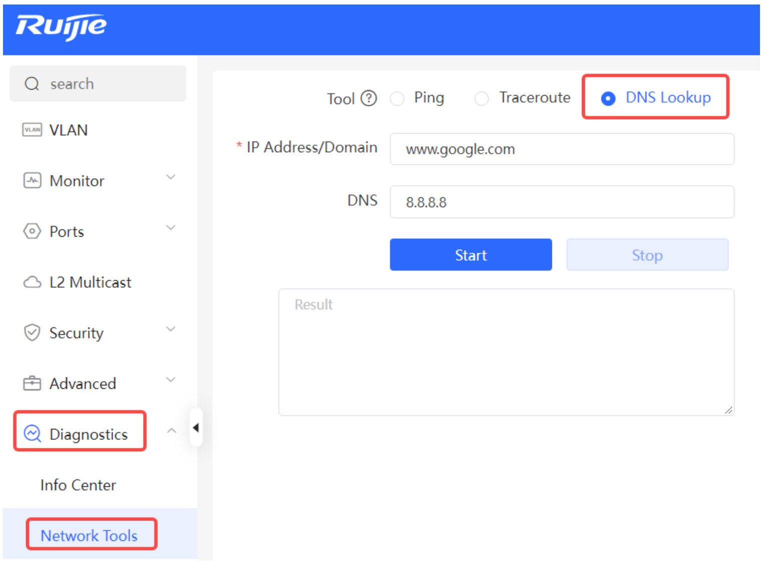
* Max TTL: 20

11.2.3 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**.



Tool ○ Ping ○ Traceroute ● DNS Lookup

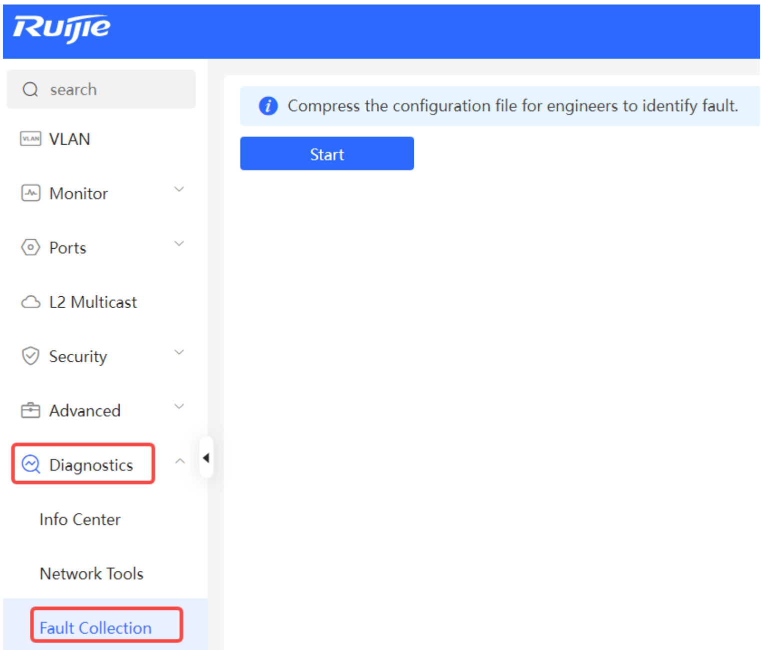
* IP Address/Domain: www.google.com

DNS: 8.8.8.8

11.3 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.



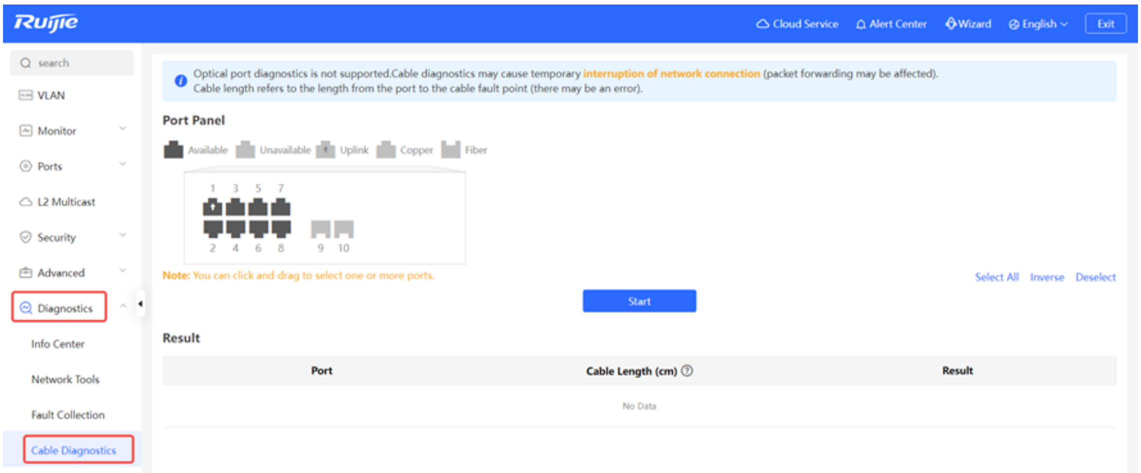
Compress the configuration file for engineers to identify fault.

11.4 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.



Optical port diagnostics is not supported.Cable diagnostics may cause temporary interruption of network connection (packet forwarding may be affected).
Cable length refers to the length from the port to the cable fault point (there may be an error).

Port Panel

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

Result

Port	Cable Length (cm) ⓘ	Result
	No Data	

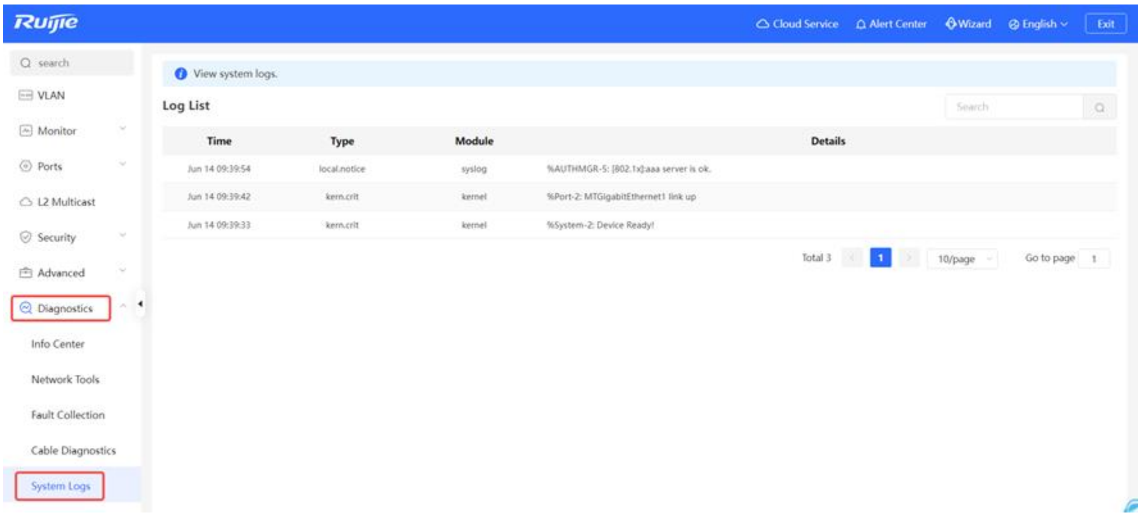
Caution

- 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.

11.5 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.



View system logs.

Log List

Time	Type	Module	Details
Jun 14 09:39:54	local.notice	syslog	%AUTHMGR-5: [802.1x]:aaa server is ok.
Jun 14 09:39:42	kern.crit	kernel	%Port-2: MTGigabitEthernet1 link up
Jun 14 09:39:33	kern.crit	kernel	%System-2: Device Ready!

11.6 Alerts

Choose **Local Device** > **Diagnostics** > **Alerts**.

Note

Click an alert in the **Alert Center** to view the faulty device, problem details, and description.

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.

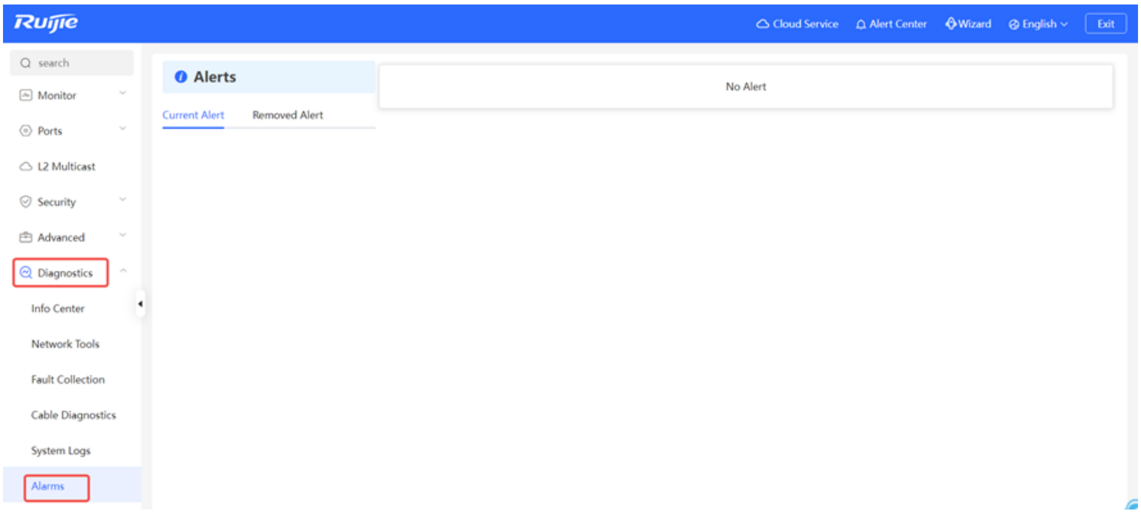


Table 11-1 Alert Types and Product Support

Alert Type	Description	Support Description
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.	N/A
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.	N/A
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of the product.	N/A
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	N/A
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".)

Alert Type	Description	Support Description
The device has a loop alarm.	A network loop occurs on the LAN.	N/A

⚠ **Caution**

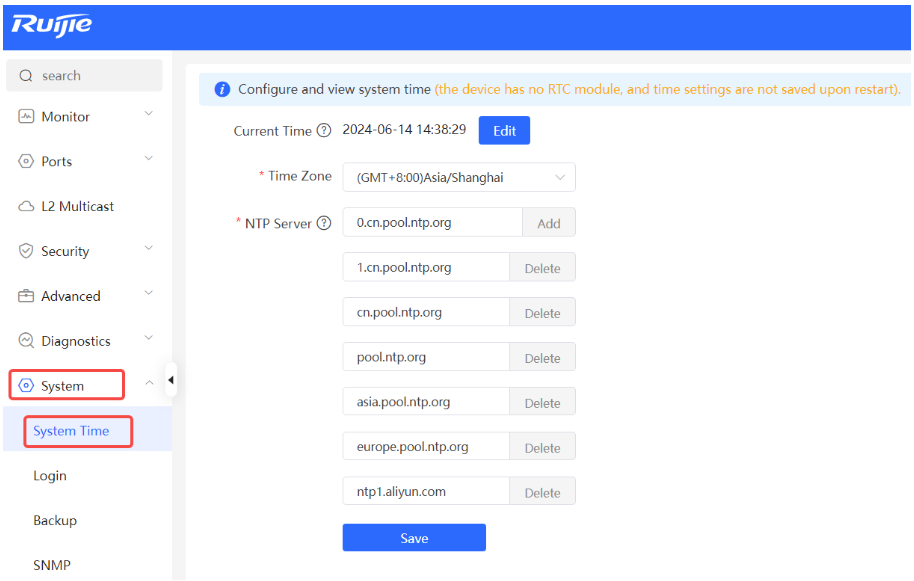
If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

12 System Configuration

12.1 Setting the System Time

Choose **Local Device** > **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, and time settings are not saved upon restart).

Current Time 2024-06-14 14:38:29

* Time Zone (GMT+8:00)Asia/Shanghai

* NTP Server 0.cn.pool.ntp.org

1.cn.pool.ntp.org

cn.pool.ntp.org

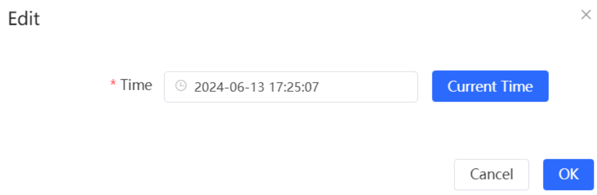
pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

ntp1.aliyun.com

Click **Current Time** when modifying the time, and the system time of the currently logged-in device will be automatically filled in.



* Time 2024-06-13 17:25:07

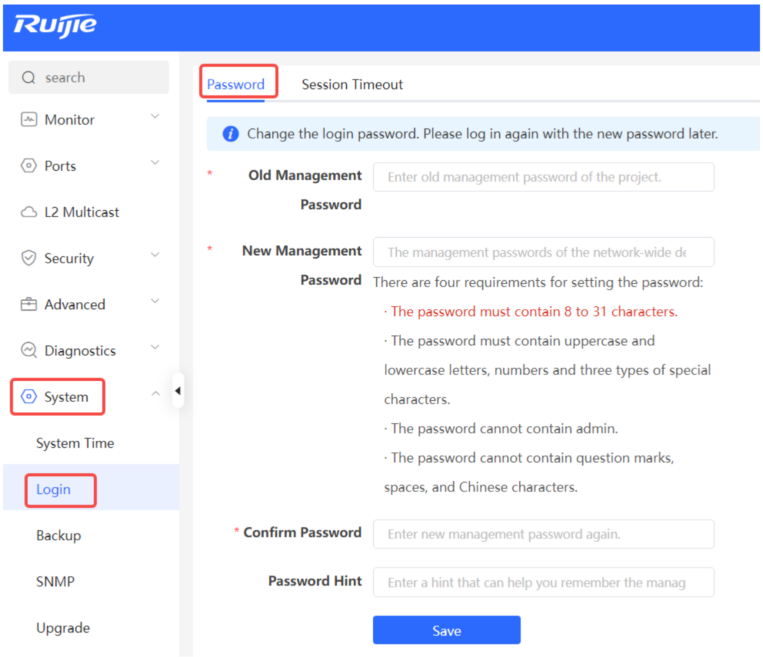
12.2 Setting the Web Login Password

Choose **Local Device** > **System** > **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 on the network will be changed synchronously.



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

* Old Management Password: Enter old management password of the project.

* New Management Password: The management passwords of the network-wide de

There are four requirements for setting the password:

- The password must contain 8 to 31 characters.
- The password must contain uppercase and lowercase letters, numbers and three types of special characters.
- The password cannot contain admin.
- The password cannot contain question marks, spaces, and Chinese characters.

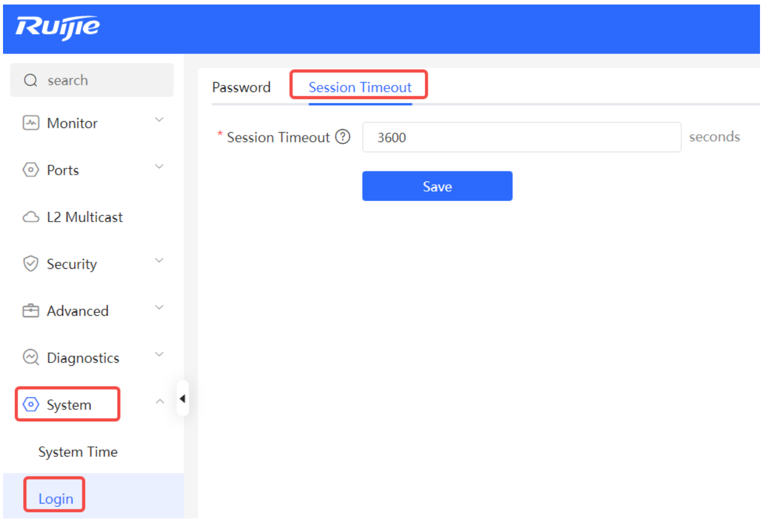
* Confirm Password: Enter new management password again.

Password Hint: Enter a hint that can help you remember the manag

12.3 Setting the Session Timeout Duration

Choose **Local Device** > **System** > **Login** > **Session Timeout**.

If you do not log out after login, the web interface allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the web interface automatically refreshes the page and you need to log in again before continuing your operations. You can change the session timeout duration.



* Session Timeout: 3600 seconds

12.4 Configuring SNMP

12.4.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

12.4.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

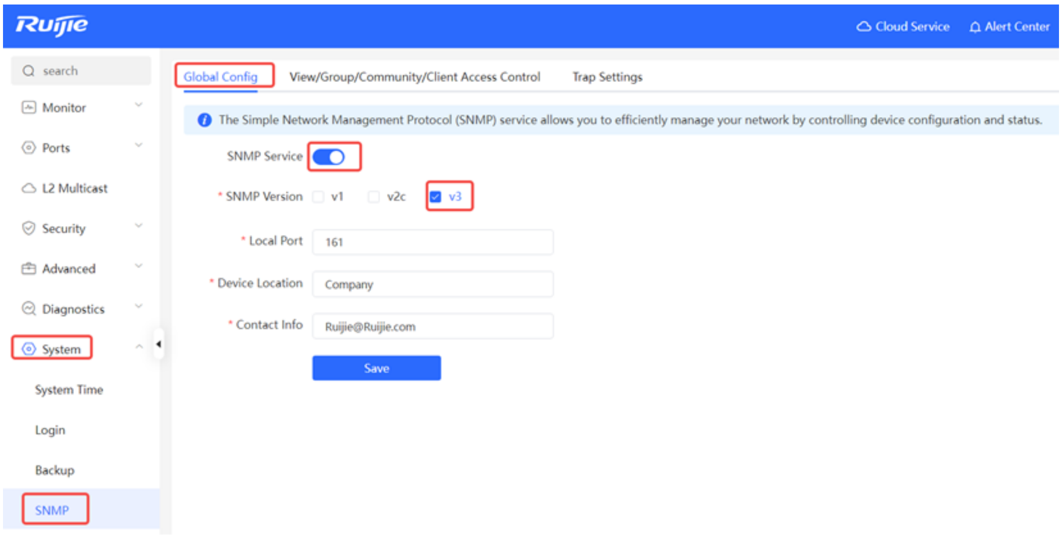
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **Global Config**

(1) Enable the SNMP service.



The Simple Network Management Protocol (SNMP) service allows you to efficiently manage your network by controlling device configuration and status.

SNMP Service: ●

* SNMP Version: □ v1 □ v2c ☑ v3

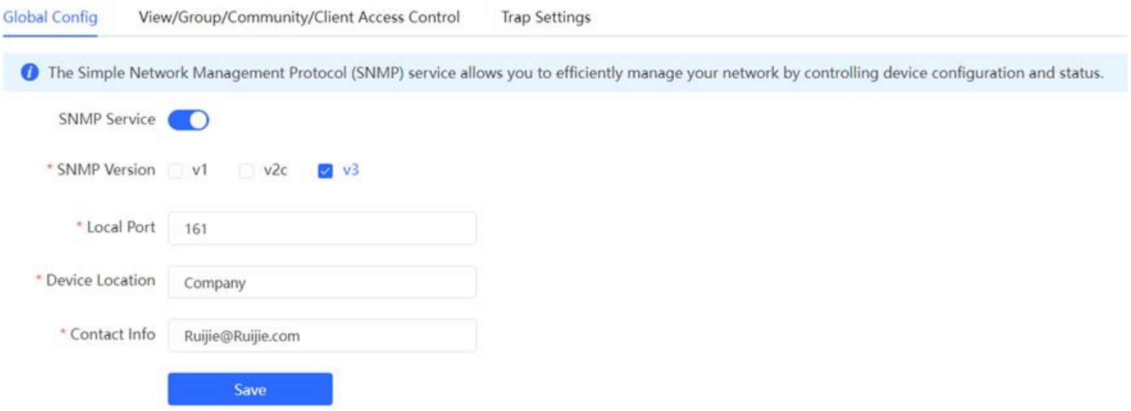
* Local Port: 161

* Device Location: Company

* Contact Info: Ruijie@Ruijie.com

When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.



The Simple Network Management Protocol (SNMP) service allows you to efficiently manage your network by controlling device configuration and status.

SNMP Service: on

* SNMP Version: □ v1 □ v2c ☑ v3

* Local Port: 161

* Device Location: Company

* Contact Info: Ruijie@Ruijie.com

Table 12-1 Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

(3) Click **Save**.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

12.4.3 View/Group/Community/Client Access Control

1. View/Group/Community/Client Access Control

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

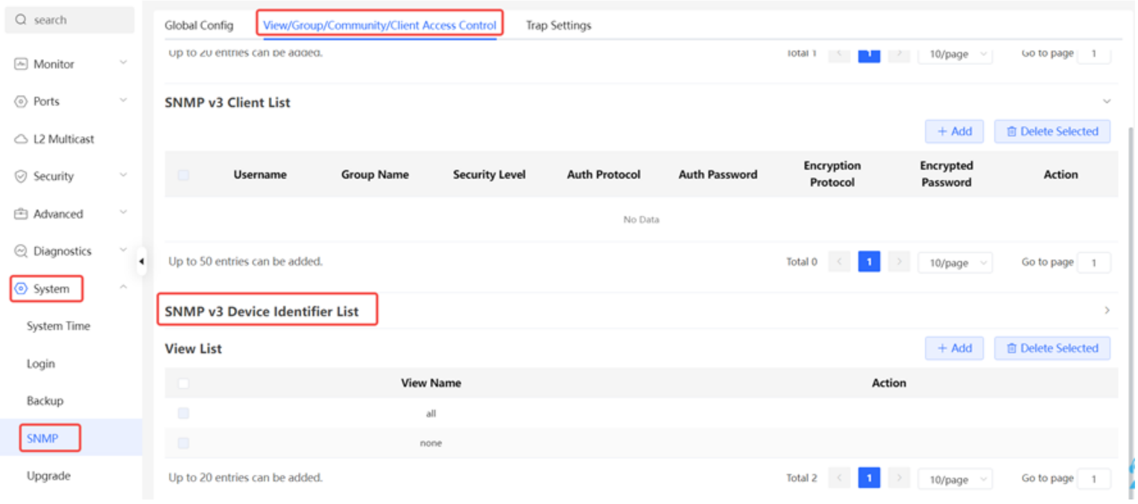
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control.**

(1) Click **Add** under the **View List** to add a view.



(2) Configure basic information of a view.

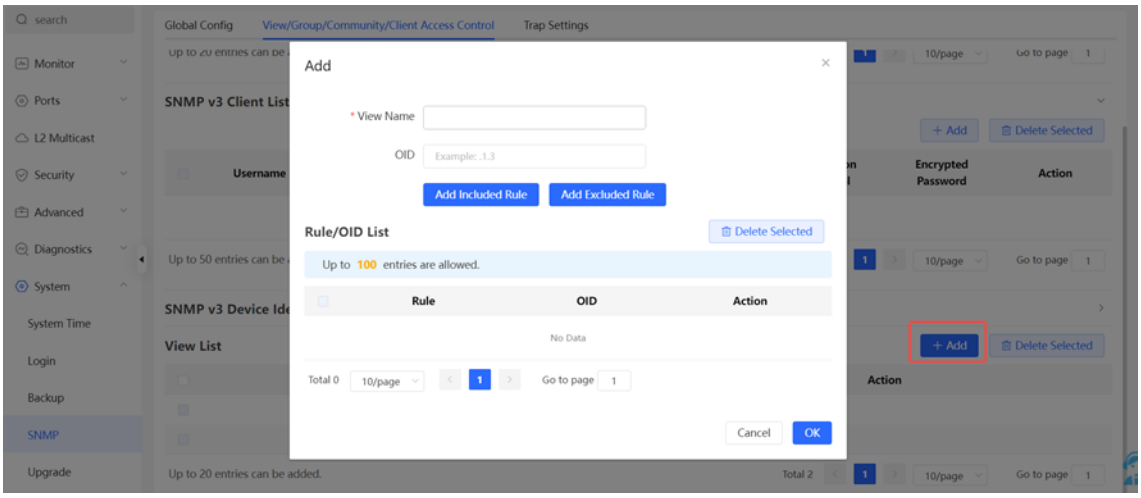


Table 12-2 View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.
Type	There are two types of rules: included and excluded rules. ● The included rule only allows access to OIDs within the OID range. Click **Add Included Rule** to set this type of view. ● Excluded rules allow access to all OIDs except those in the OID range. Click **Add Excluded Rule** to configure this type of view.

Note

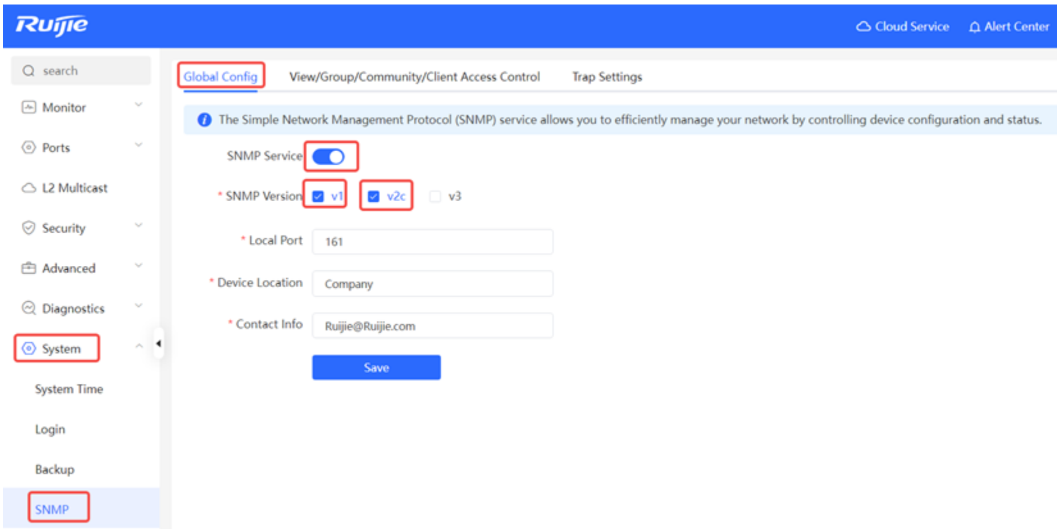
At least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

When the SNMP version is set to v1/v2c, user configuration is required.



The Simple Network Management Protocol (SNMP) service allows you to efficiently manage your network by controlling device configuration and status.

SNMP Service: on

* SNMP Version: ☑ v1 ☑ v2c □ v3

* Local Port: 161

* Device Location: Company

* Contact Info: Ruijie@Ruijie.com

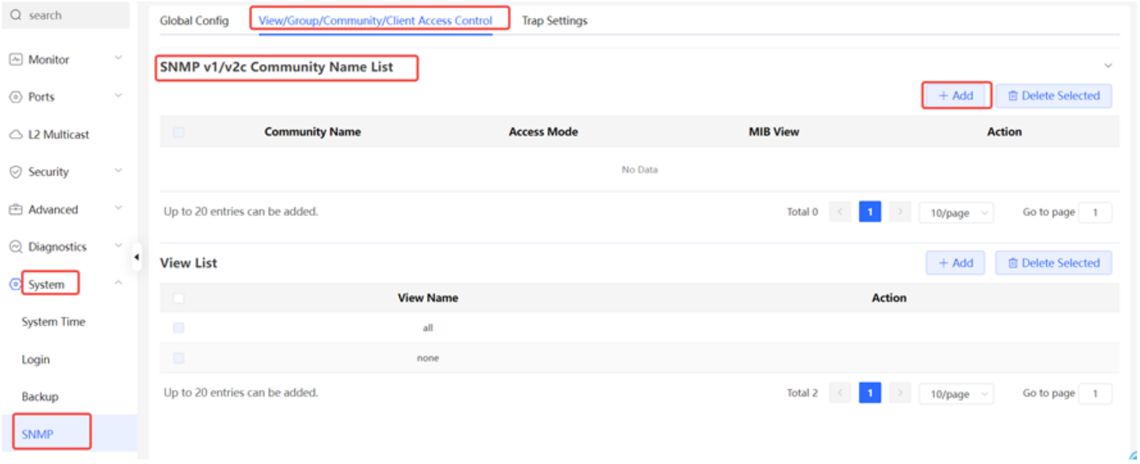
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control.**

(1) Click **Add** in the SNMP v1/v2c Community Name List pane.



SNMP v1/v2c Community Name List

□	Community Name	Access Mode	MIB View	Action
	No Data			

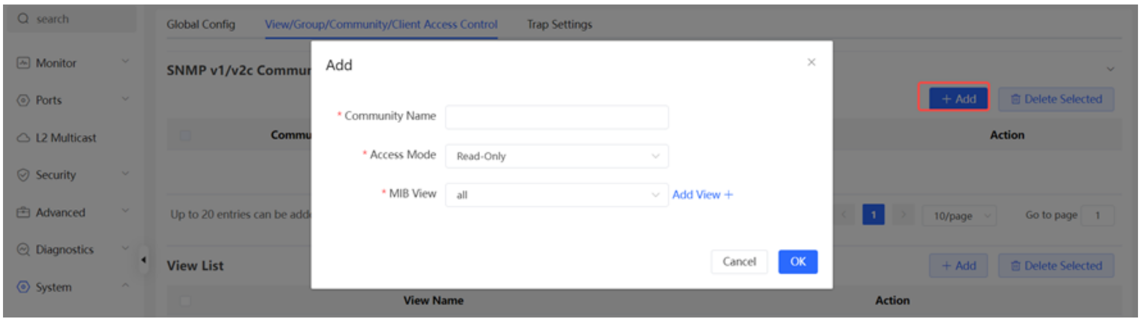
Up to 20 entries can be added. Total 0 1 10/page Go to page 1

View List

□	View Name	Action
□	all	
□	none	

Up to 20 entries can be added. Total 2 1 10/page Go to page 1

(2) Add a v1/v2c user.



Add

* Community Name

* Access Mode Read-Only

* MIB View all Add View +

Cancel OK

Table 12-3 v1/v2c User Configuration Parameters

Parameter	Description
Community Name	At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Access Mode	Indicates the access permission (read-only or read & write) for the community name.
MIB View	The options under the drop-down box are configured views (default: all, none).

⚠ Note

- Community names cannot be the same among v1/v2c users.
- Click **Add View** to add a view.

3. Configuring v3 Groups

- Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

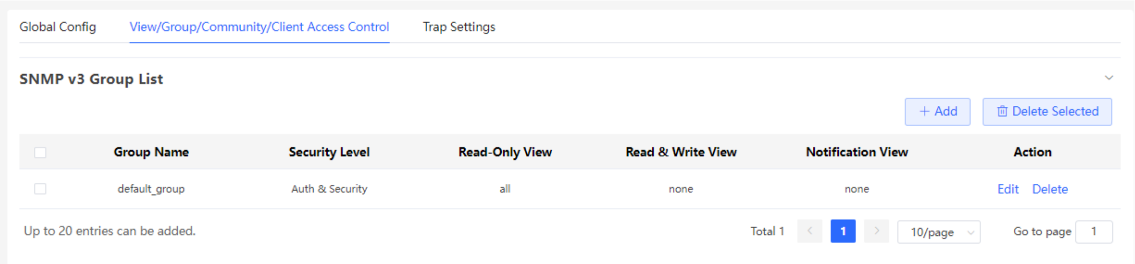
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System > SNMP** > **View/Group/Community/Client Access Control**.

(1) Click **Add** in the SNMP v3 Group List pane to create a group.

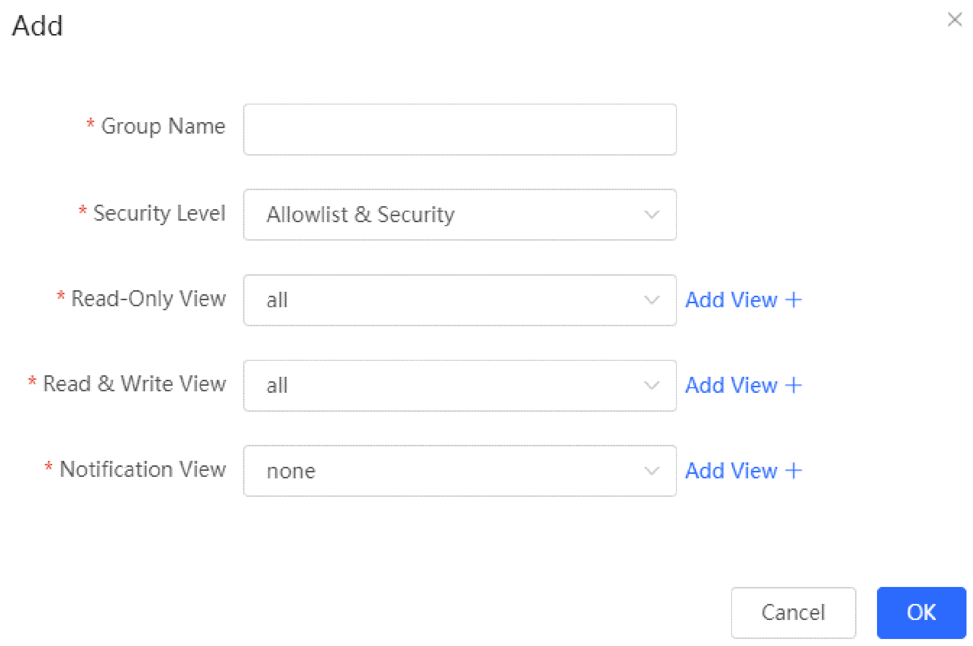


SNMP v3 Group List

□	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
□	default_group	Auth & Security	all	none	none	Edit Delete

Up to 20 entries can be added.

(2) Configure v3 group parameters.



Add

* Group Name

* Security Level: Allowlist & Security

* Read-Only View: all

* Read & Write View: all

* Notification View: none

Table 12-4 v3 Group Configuration Parameters

Parameter	Description
Group Name	Indicates the name of the group. 1-32 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notify View	The options under the drop-down box are configured views (default: all, none).

Note

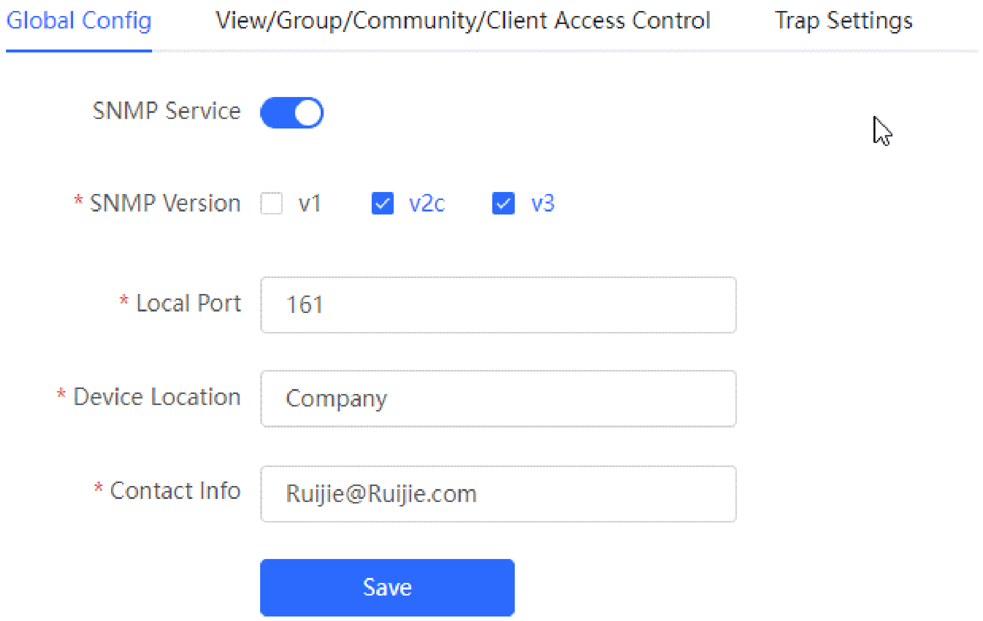
- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.



SNMP Service: On

* SNMP Version: □ v1 ☑ v2c ☑ v3

* Local Port: 161

* Device Location: Company

* Contact Info: Ruijie@Ruijie.com

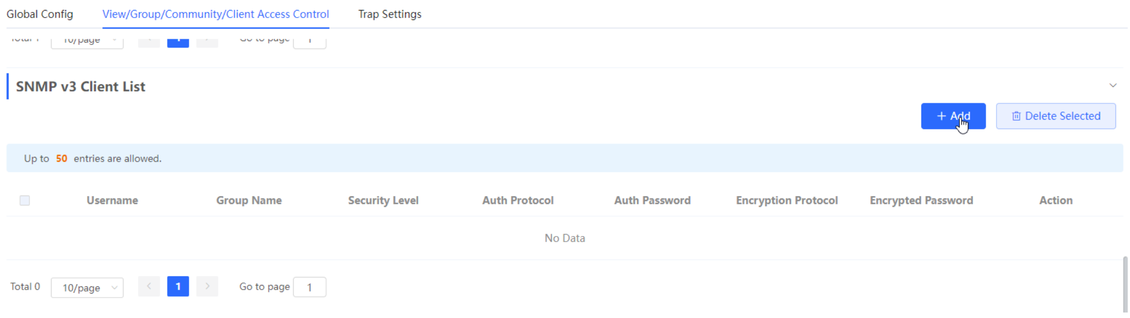
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System > SNMP** > **View/Group/Community/Client Access Control**

(1) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.



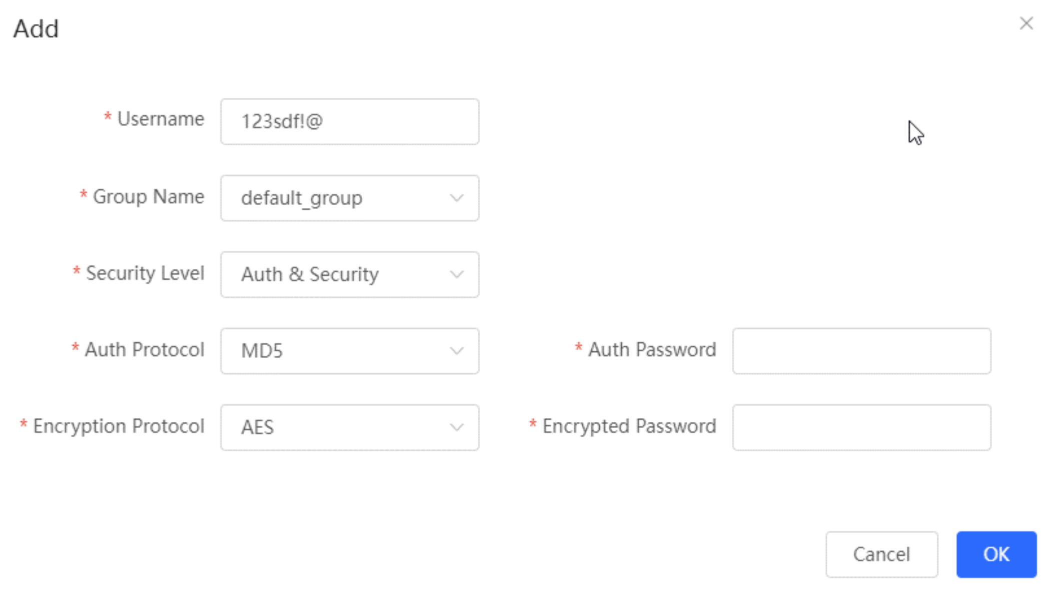
SNMP v3 Client List

Up to 50 entries are allowed.

□	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
No Data								

Total 0 10/page < 1 > Go to page 1

(2) Configure v3 user parameters.



Add

* Username: 123sdf!@

* Group Name: default_group

* Security Level: Auth & Security

* Auth Protocol: MD5

* Auth Password:

* Encryption Protocol: AES

* Encrypted Password:

Table 12-5 v3 User Configuration Parameters

Parameter	Description
Username	Username At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase

Parameter	Description
	and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

⚠ **Note**

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

12.4.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

- Configuration Specification

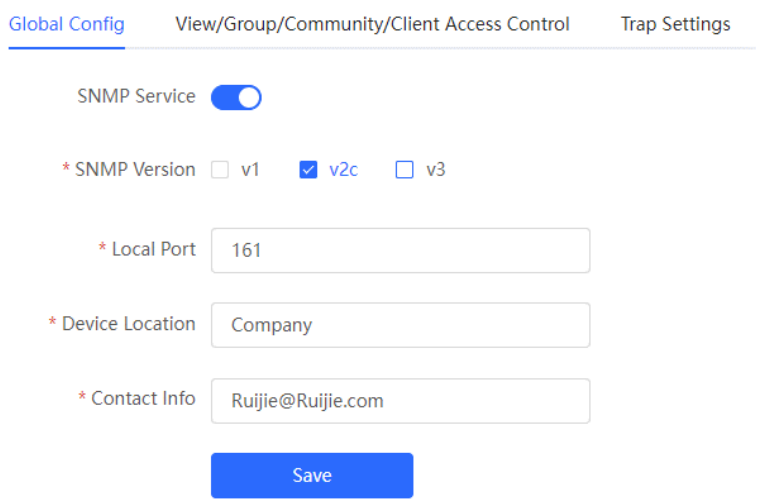
According to the user's application scenario, the requirements are shown in the following table:

Table 12-6 User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "public", and the default port number is 161.
Read & write permission	Read-only permission.

- Configuration Steps

(1) Choose **Local Device** > **System** > **SNMP** > **Global Config**, select v2c and set other settings as default. Then, click **Save**.



SNMP Service: on

* SNMP Version: □ v1 ☑ v2c □ v3

* Local Port: 161

* Device Location: Company

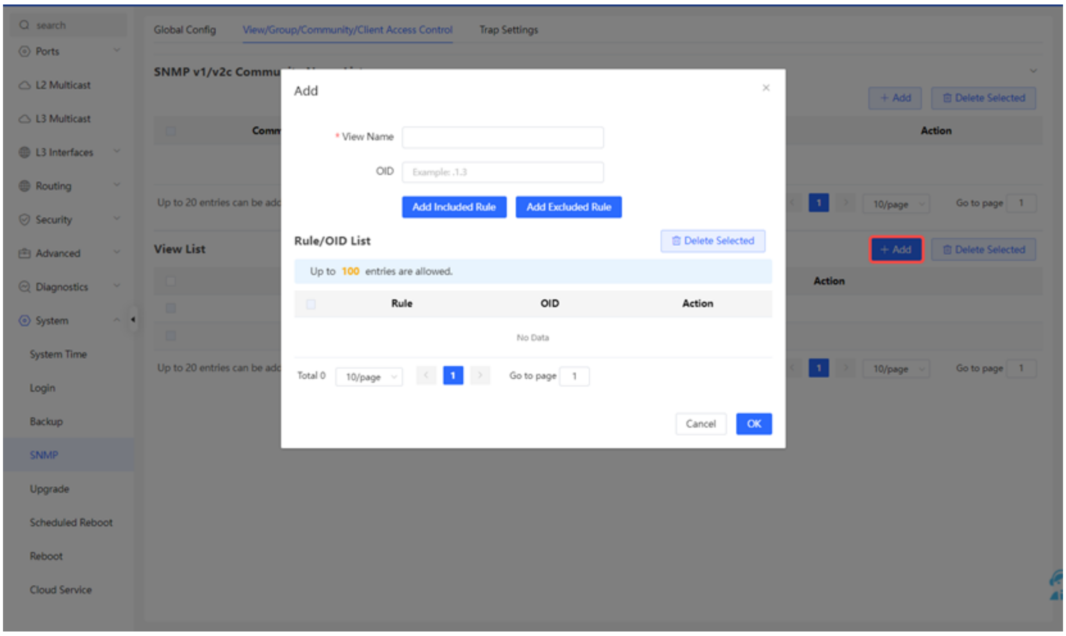
* Contact Info: Ruijie@Ruijie.com

(2) Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control** ,Add a view on the View/Group/Community/Client Access Control interface.

a Click **Add** in the **View List** pane.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

c Click **OK**.



Add

* View Name

OID Example: .1.3

Rule/OID List

Up to 100 entries are allowed.

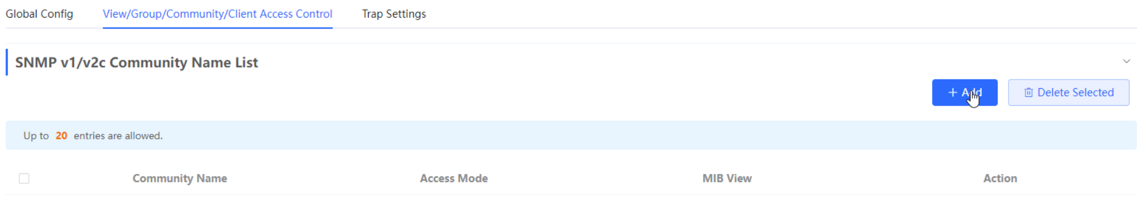
□	Rule	OID	Action

No Data

Total 0 10/page 1 Go to page 1

Up to 20 entries can be add

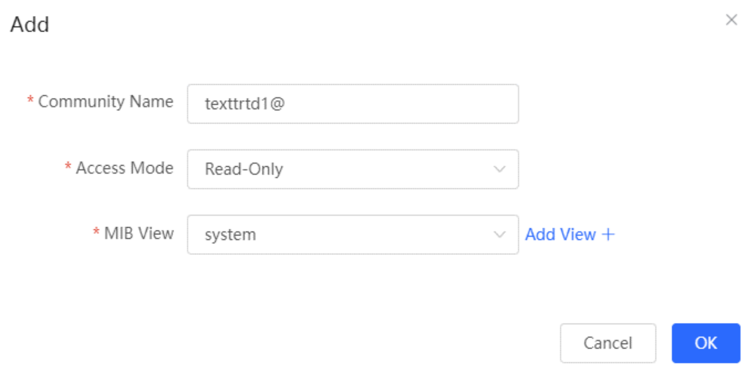
(3) Click **Add** in the SNMP v1/v2c community name list, fill in the community name, access mode and view in the pop-up window, and click **OK** after the operation is completed.



SNMP v1/v2c Community Name List

Up to 20 entries are allowed.

□	Community Name	Access Mode	MIB View	Action



Add

* Community Name: texttrtd1@

* Access Mode: Read-Only

* MIB View: system

2. v3 version SNMP service configuration

- Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

- Configuration Specification

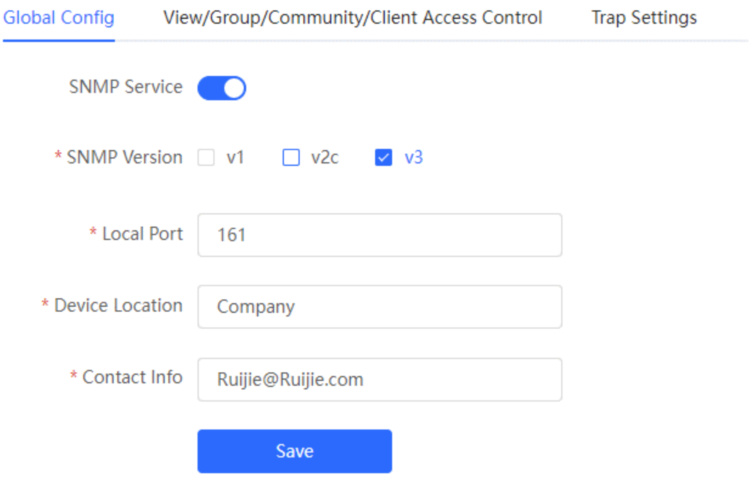
According to the user's application scenario, the requirements are shown in the following table:

Table 12-7 User Requirements Description Form

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

(1) Choose **Local Device** > **System** > **SNMP** > **Global Config**, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.



Global Config | View/Group/Community/Client Access Control | Trap Settings

SNMP Service: ●

* SNMP Version: □ v1 □ v2c ☑ v3

* Local Port: 161

* Device Location: Company

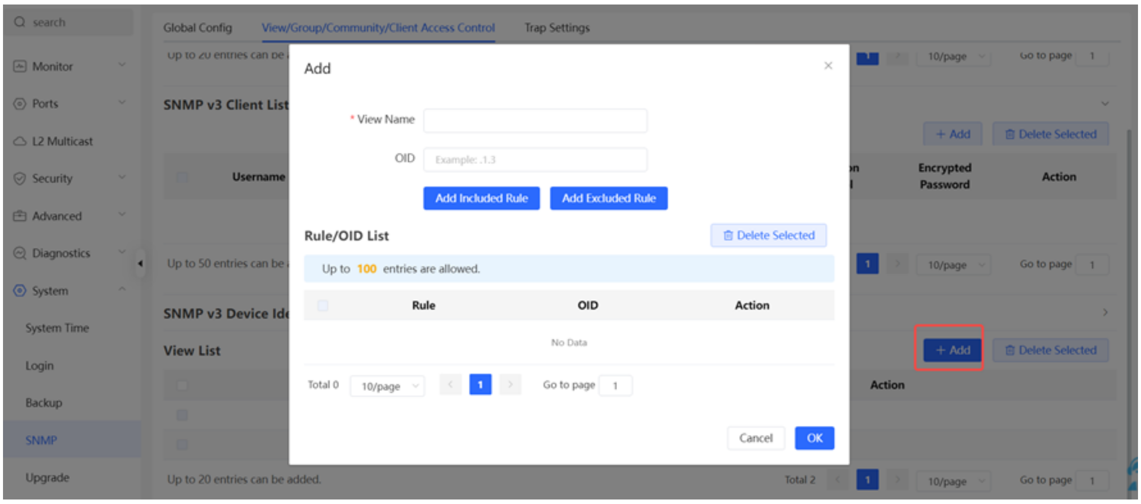
* Contact Info: Ruijie@Ruijie.com

(2) Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control**. Add a view on the View/Group/Community/Client Access Control interface.

a Click **Add** in the **View List** pane.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

c Click **OK**.



Add

* View Name:

OID: Example: .1.3

Rule/OID List

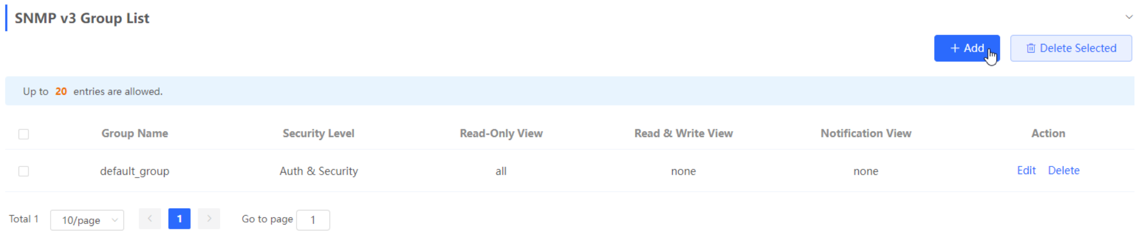
Up to 100 entries are allowed.

Rule	OID	Action
No Data		

Total 0 10/page 1 Go to page 1

Up to 20 entries can be added. Total 2

(3) Click **Add** in the SNMP v3 group list, fill in the group name and security level in the pop-up window, the user has read and write permissions, select "public _view" for the readable view and read and write view, and set the notification view to none. After the operation is complete, click **OK**.

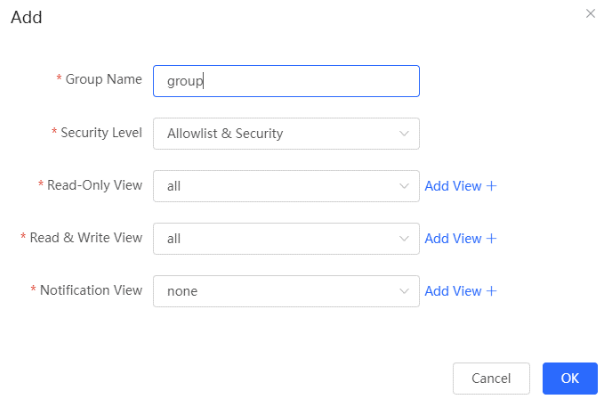


SNMP v3 Group List

Up to 20 entries are allowed.

□	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
□	default_group	Auth & Security	all	none	none	Edit Delete

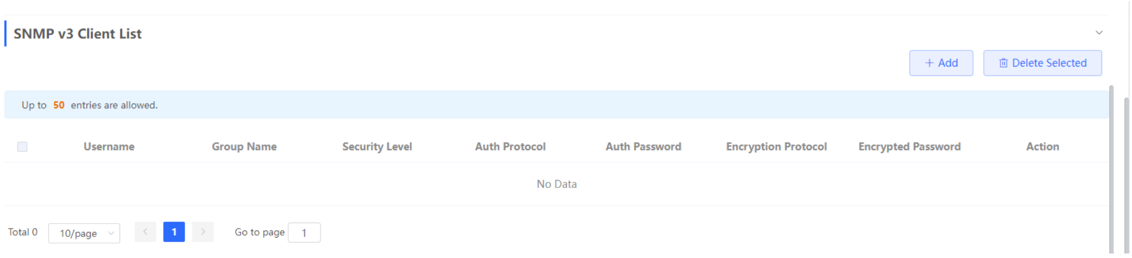
Total 1 10/page 1 Go to page 1



Add

- * Group Name: group
- * Security Level: Allowlist & Security
- * Read-Only View: all
- * Read & Write View: all
- * Notification View: none

(4) Click Add in the SNMP v3 user list, fill in the user name and group name in the pop-up window, the user security level adopts authentication and encryption mode, fill in the corresponding authentication protocol, authentication password, encryption protocol, and encryption password, and click **OK**.



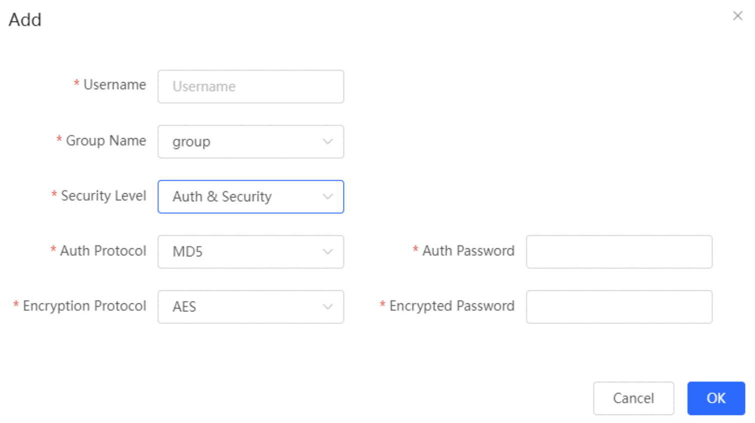
SNMP v3 Client List

Up to 50 entries are allowed.

□	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action

No Data

Total 0 10/page 1 Go to page 1



Add

- * Username: Username
- * Group Name: group
- * Security Level: Auth & Security
- * Auth Protocol: MD5
- * Auth Password:
- * Encryption Protocol: AES
- * Encrypted Password:

12.4.5 Trap service configuration

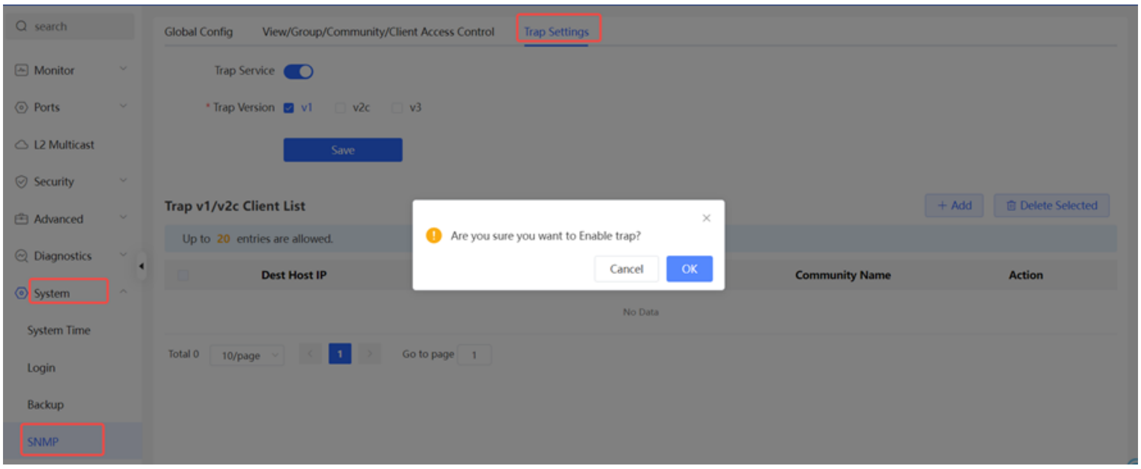
Trap is a notification mechanism of the SNMP (Simple Network Management Protocol) protocol, which is used to report the status and events of network devices to managers, including device status reports, fault reports, performance reports, configuration reports and security management. Trap can provide real-time network monitoring and fault diagnosis to help administrators find and solve network problems in time.

1. Trap open settings

Enable the trap service and select the effective trap protocol version, including v1, v2c, and v3.

Choose **Local Device** > **System > SNMP** > **Trap setting**

(1) Enable the trap service switch.



Trap Service: on

* Trap Version: ☑ v1 □ v2c □ v3

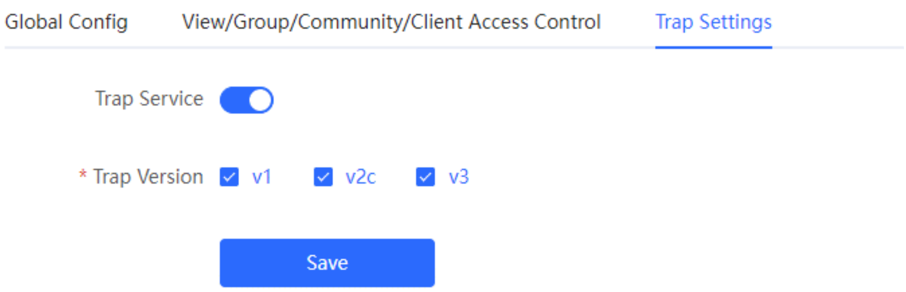
Trap v1/v2c Client List

Up to 20 entries are allowed.

Are you sure you want to Enable trap?

No Data

When the first open is turned on, the system pops up a prompt message. Click **OK**.



Trap Service: on

* Trap Version ☑ v1 ☑ v2c ☑ v3

(2) Set the trap version.

The trap protocol version number includes v1 version, v2c version, and v3 version.

(3) Click **OK**.

After the trap service is enabled, you need to click **Save**, and the configuration of the trap protocol version number will take effect.

2. Trap v1/v2c user configuration

- Introduction

A trap is a notification mechanism used to send an alert to administrators when important events or failures occur on a device or service. Trap v1/v2c are two versions of SNMP protocol, used for network management and monitoring.

Trap v1 is the first version in the SNMP protocol, which supports basic alarm notification functions. trap v2c is the second version in the SNMP protocol, which supports more alarm notification options and more advanced security.

By using trap v1/v2c, the administrator can know the problems on the network in time and take corresponding measures.

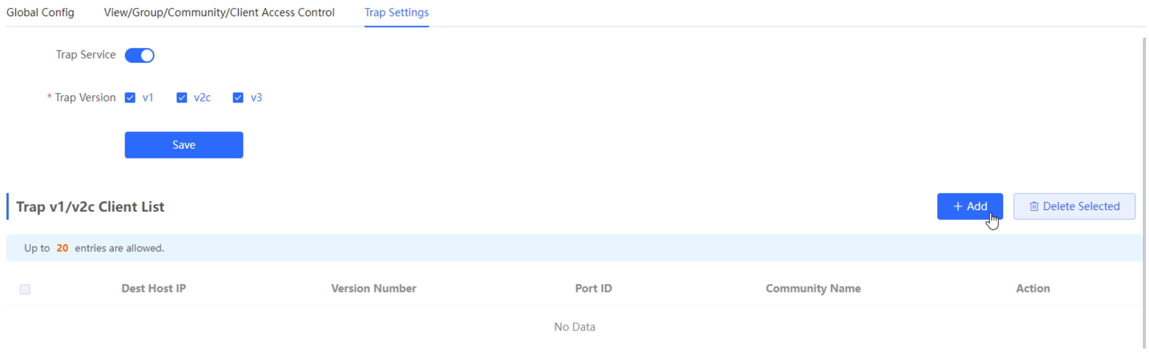
- Prerequisites

When the trap service version selects v1 or v2c, a trap v1v2c user needs to be created.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **Trap setting**.

(1) Click Add in the Trap v1v2c User list to create a trap v1v2c user.



Trap Service

* Trap Version ☑ v1 ☑ v2c ☑ v3

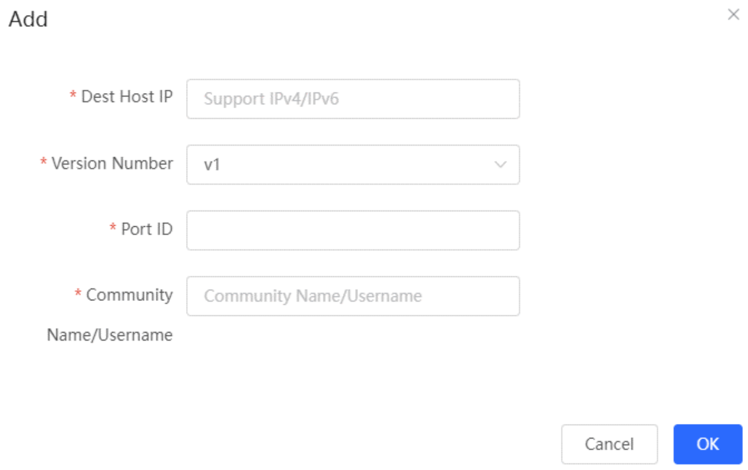
Trap v1/v2c Client List

Up to 20 entries allowed.

□	Dest Host IP	Version Number	Port ID	Community Name	Action

No Data

(2) Configure trap v1v2c user-related parameters.



Add

* Dest Host IP: Support IPv4/IPv6

* Version Number: v1

* Port ID:

* Community Name/Username: Community Name/Username

Table 12-8 Trap v1/v2c user information description table

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
Community name/User name	Community name of the trap user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.

⚠ **Note**

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/ v1/v2c users cannot be the same.

(3) Click **OK**.

3. trap v 3 user configuration

- Introduction

Trap v3 is a network management mechanism based on SNMP protocol, which is used to send alarm notifications to management personnel. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption.

Trap v3 can be customized to choose the conditions and methods to send alerts, as well as who receives alerts and how to be notified. This enables administrators to understand the status of network devices more accurately and take timely measures to ensure network security and reliability.

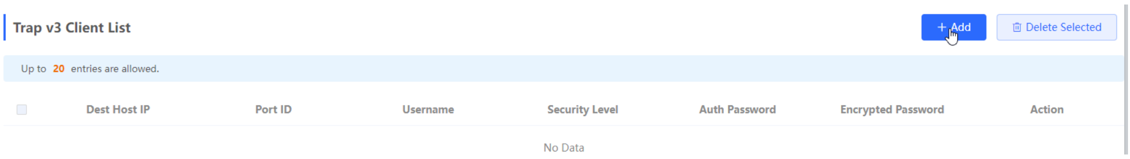
- Prerequisites

When v3 is selected as the trap service version, a trap v3 user needs to be created.

- Configuration Steps

Choose **Local Device** > **System > SNMP** > **Trap setting**.

(1) Click Add in the "Trap v3 user" list to create a trap v3 user.



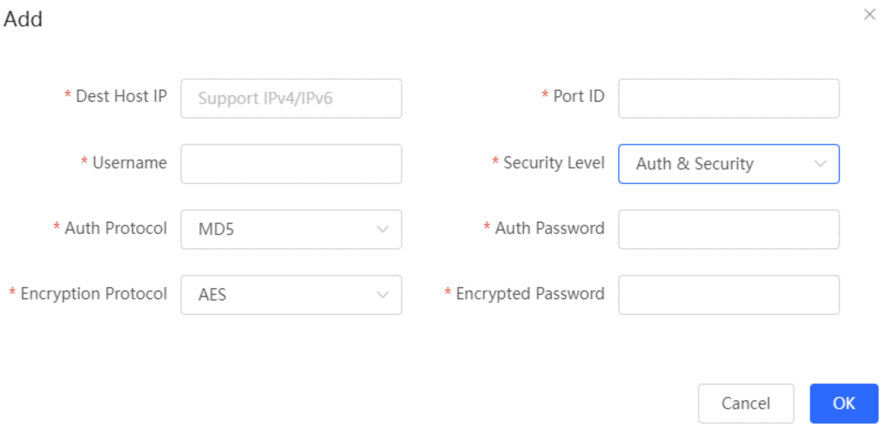
Trap v3 Client List

Up to 20 entries are allowed.

□	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action

No Data

(2) Configure parameters related to t rap v3 users.



Add

* Dest Host IP: Support IPv4/IPv6
* Port ID:
* Username:
* Security Level: Auth & Security
* Auth Protocol: MD5
* Auth Password:
* Encryption Protocol: AES
* Encrypted Password:

Table 12-9 trap v3 user information description table

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed.

Parameter	Description
	Question marks, spaces, and Chinese characters are not allowed.
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

⚠ **Note**

IP of t rap v1/v2c/v3 users cannot be repeated.

12.4.6 Typical configuration examples of the trap service

1. v2c version trap configuration

- Application Scenarios

When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, so configure the device with the destination ip 1 92.1 68.110.85 and port number 1 66, so that the device sends a trap of the v2c version in case of an exception.

- Configuration Specification

According to the analysis of the user's usage scenario, the requirements are shown in the table:

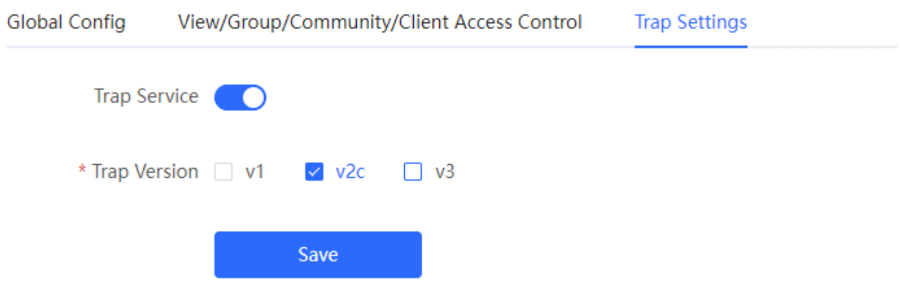
Table 12-10 User Requirements Description Form

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.

Item	Description
Version	Select the v2 version.
Community name/User name	Trap_user

- Configuration Steps

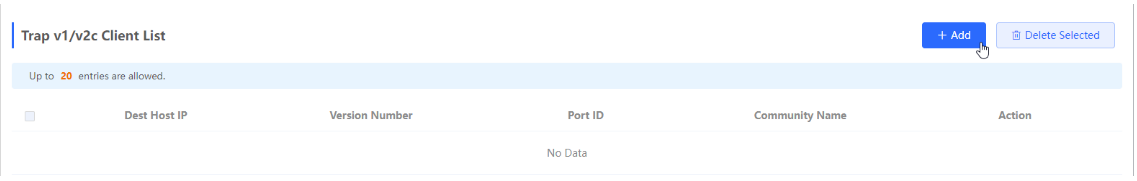
(1) Choose **Local Device** > **System** > **SNMP** > **Trap setting**. Select the v2c version on the trap setting interface, click **Save**.



Trap Service

* Trap Version □ v1 ☑ v2c □ v3

(2) Click Add in the "trap v1 / v2c user list".

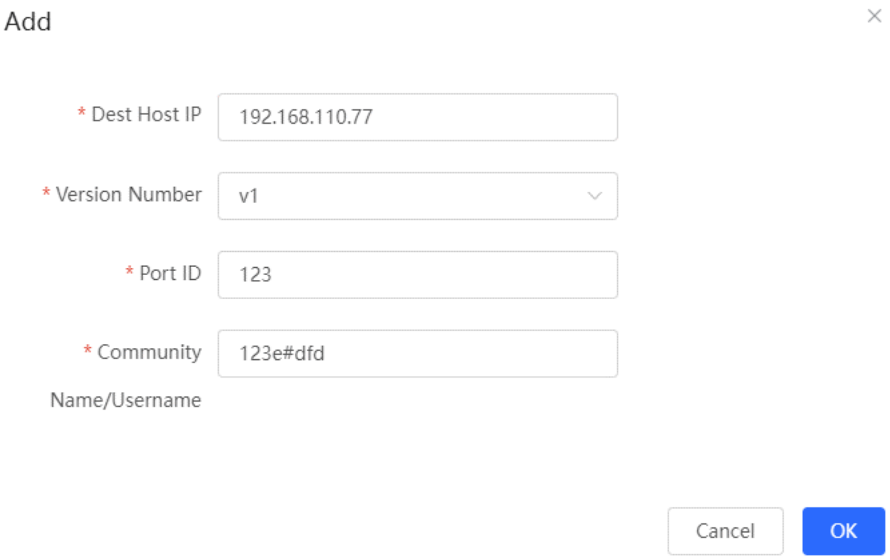


Trap v1/v2c Client List

Up to 20 entries are allowed.

□	Dest Host IP	Version Number	Port ID	Community Name	Action
No Data					

(3) Fill in the target host IP, version number, port number, user name and other information, and click OK after the configuration is complete.



* Dest Host IP: 192.168.110.77

* Version Number: v1

* Port ID: 123

* Community Name/Username: 123e#dfd

2. V3 version trap configuration

- Application Scenarios

When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, and the device with the destination ip of 1 92.1 68.110.87 and the port number of 1 67 is configured, and use the more secure v3 version to send traps.

- Configuration Specification

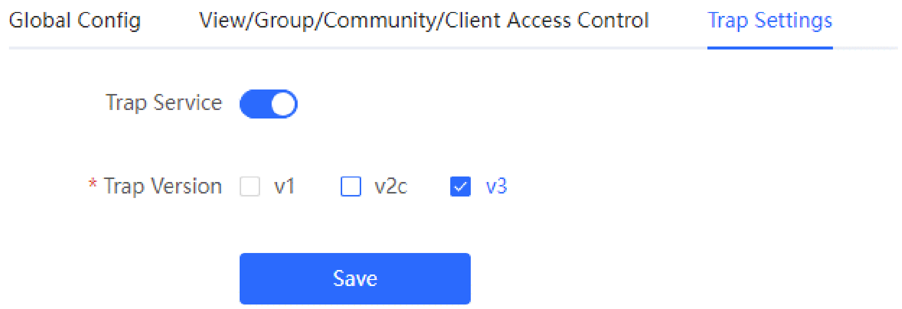
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 12-11 User Requirements Description Form

Item	Description
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_user for the user name.
Authentication protocol/authentication password Encryption protocol/encryption password	Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123

- Configuration Steps

(1) Select the v3 version on the trap setting interface, and click **Save**.

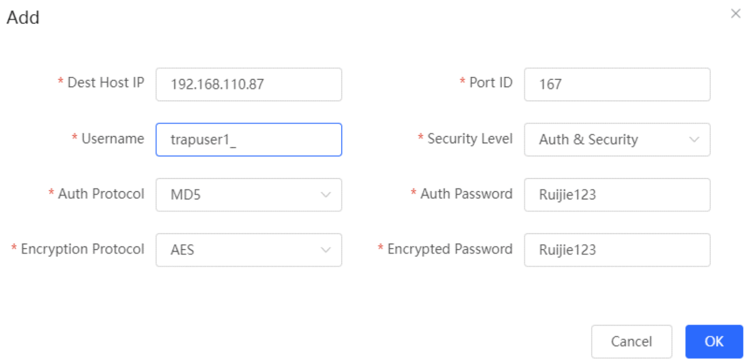


Trap Service ●

* Trap Version □ v1 □ v2c ☑ v3

(2) Click Add in the trap v3 user list.

(3) Fill in the target host IP, port number, user name and other information, and click OK after the configuration is complete.



* Dest Host IP 192.168.110.87

* Port ID 167

* Username trapuser1_

* Security Level Auth & Security

* Auth Protocol MD5

* Auth Password Ruijie123

* Encryption Protocol AES

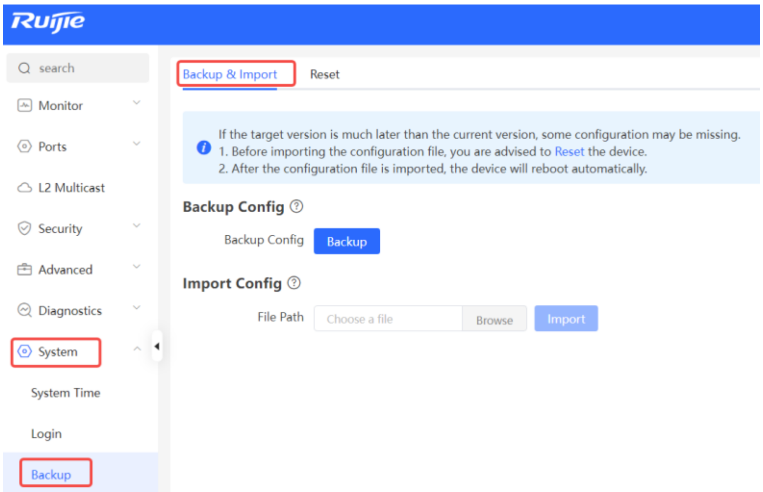
* Encrypted Password Ruijie123

12.5 Configuration Backup and Import

Choose **Local Device** > **System** > **Backup** > **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.
1. Before importing the configuration file, you are advised to Reset the device.
2. After the configuration file is imported, the device will reboot automatically.

Backup Config

Backup Config: Backup

Import Config

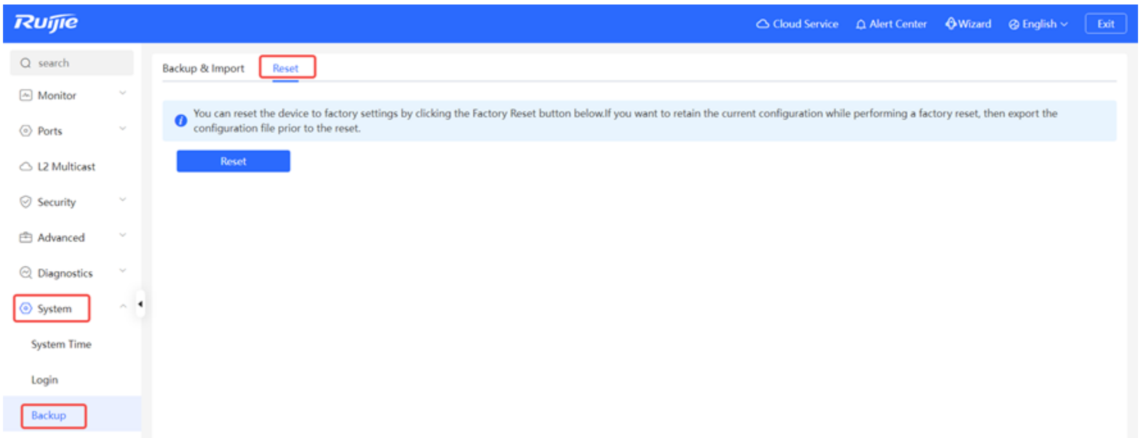
File Path: Choose a file | Browse | Import

12.6 Reset

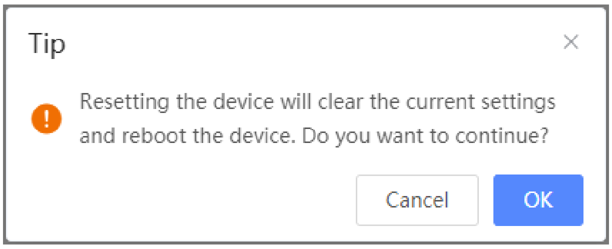
12.6.1 Resetting the Device

Choose **Local Device** > **System** > **Backup** > **Reset**.

Click **Reset**, and click **OK** to restore factory settings.



You can reset the device to factory settings by clicking the Factory Reset button below.If you want to retain the current configuration while performing a factory reset, then export the configuration file prior to the reset.



Resetting the device will clear the current settings and reboot the device. Do you want to continue?

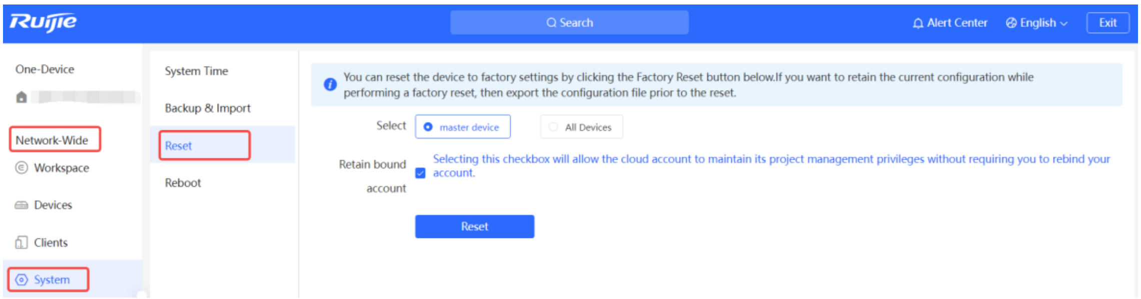
Caution

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 12.5 Configuration Backup and Import) before restoring the factory settings. Exercise caution when performing this operation.

12.6.2 Resetting the Devices on the network

Choose **Network-Wide** > **System** > **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.



You can reset the device to factory settings by clicking the Factory Reset button below.If you want to retain the current configuration while performing a factory reset, then export the configuration file prior to the reset.

Select ● master device ○ All Devices

Retain bound account ☑ Selecting this checkbox will allow the cloud account to maintain its project management privileges without requiring you to rebind your account.

Reset

Caution

Resetting the network will clear current settings of all devices on the network and reboot the devices. Exercise caution when performing this operation.

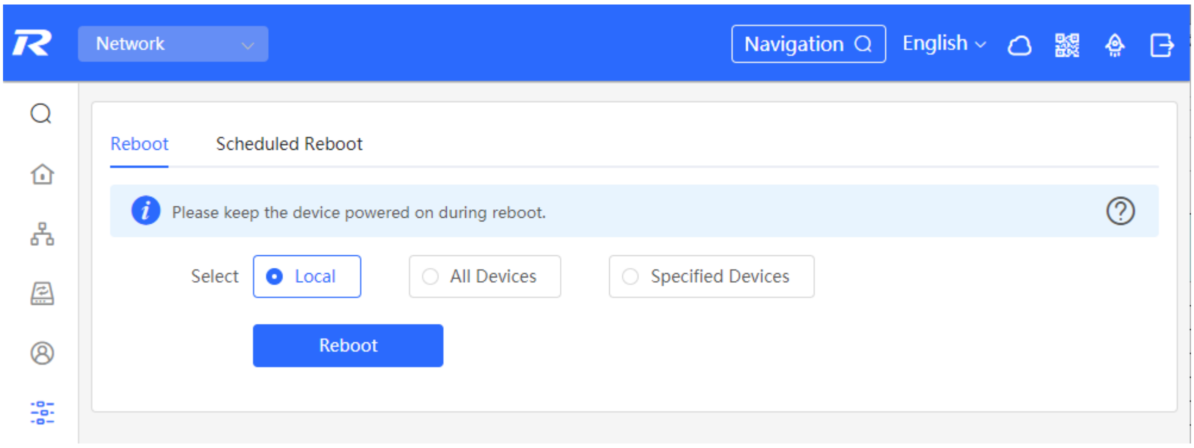
12.7 Rebooting the Device

12.7.1 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.

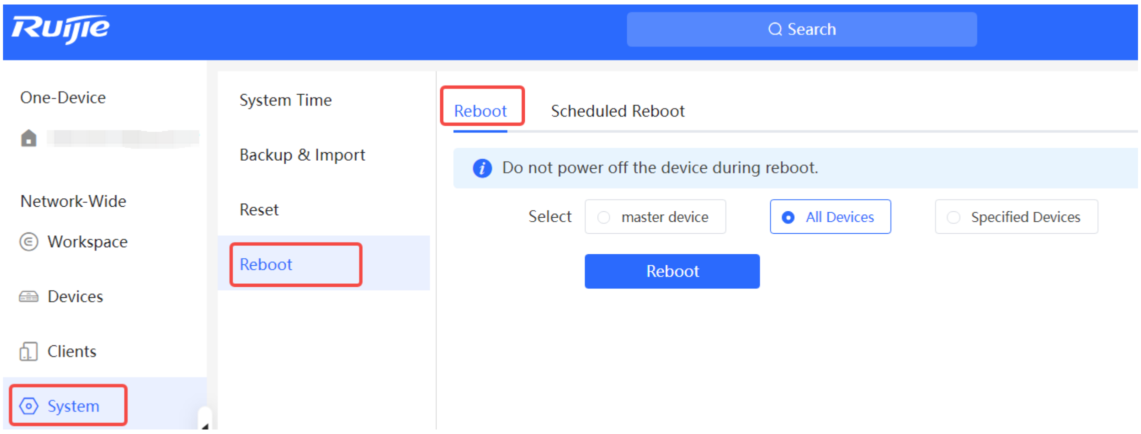
Select ● Local ○ All Devices ○ Specified Devices

Reboot

12.7.2 Rebooting the Devices on the Network

Choose **Network** > **System** > **Reboot** > **Reboot**.

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.



Do not power off the device during reboot.

Select ○ master device ● All Devices ○ Specified Devices

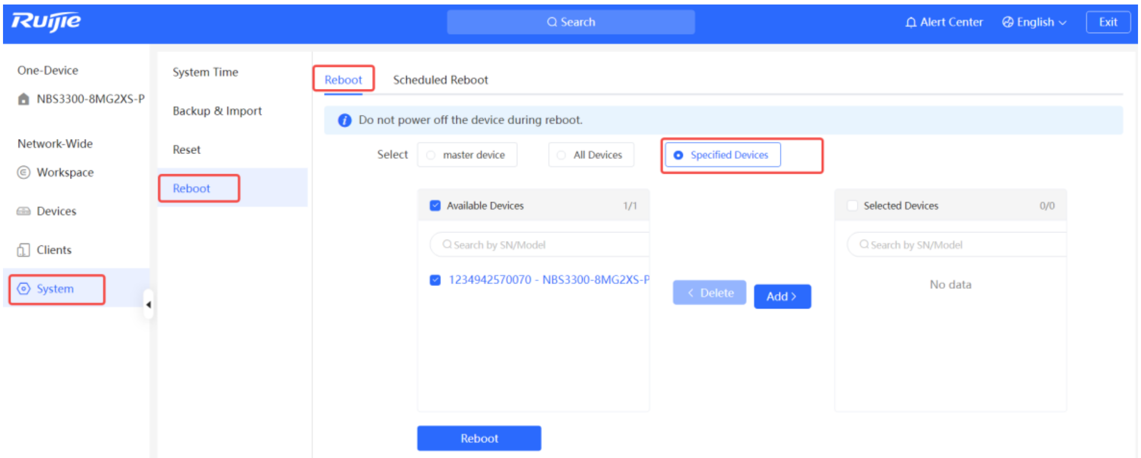
Caution

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.

12.7.3 Rebooting Specified Devices on 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.



Do not power off the device during reboot.

Select ○ master device ○ All Devices ● Specified Devices

☑ Available Devices 1/1

☑ 1234942570070 - NBS3300-8MG2XS-P

□ Selected Devices 0/0

No data

12.8 Configuring Scheduled Reboot

Confirm that the system time is accurate. For details about how to configure the system time, see 12.1 Setting the System Time. To avoid network interruption caused by device reboot at wrong time.

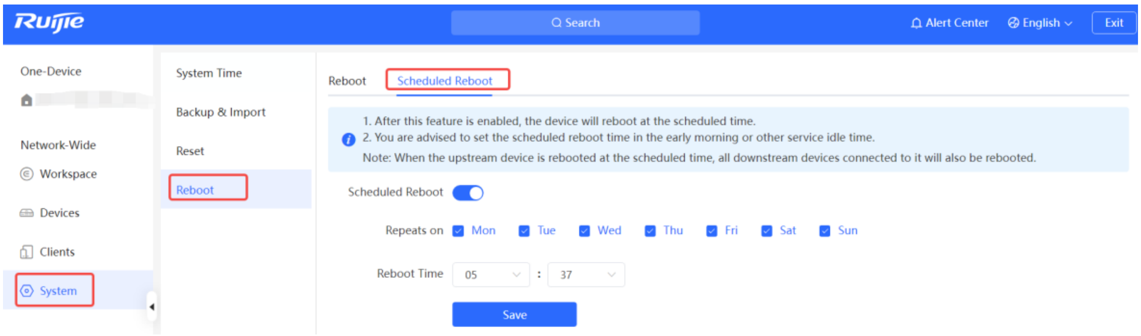
Choose **Self-Organizing Mode** > **Network** > **System** > **Scheduled Reboot**.

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 on the network mode, all devices on the network will reboot when the system time matches to the timed time. Therefore, exercise caution when performing this operation.



1. After this feature is enabled, the device will reboot at the scheduled time.
2. You are advised to set the scheduled reboot time in the early morning or other service idle time.

Note: When the upstream device is rebooted at the scheduled time, all downstream devices connected to it will also be rebooted.

Scheduled Reboot ●

Repeats on ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Reboot Time 05 : 37

12.9 Upgrade

Caution

- It is recommended to back up the configuration before software upgrade.
- Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

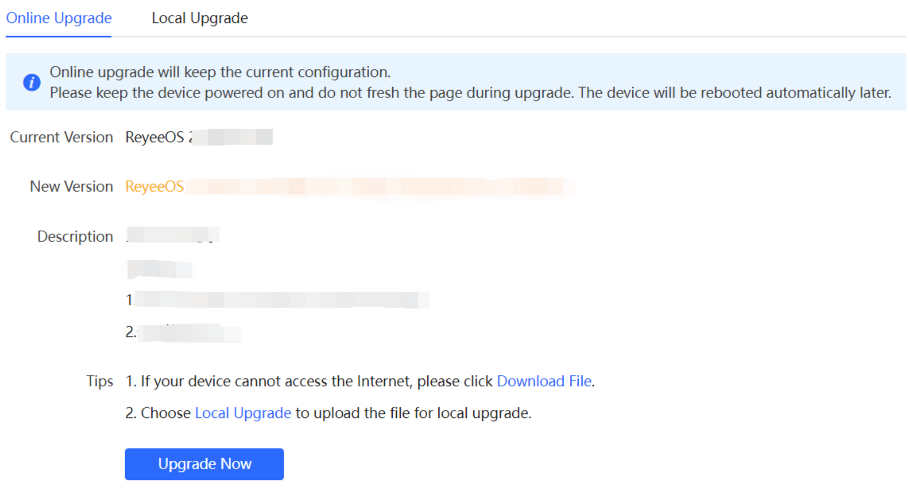
12.9.1 Online Upgrade

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 will keep the current configuration.
Please keep the device powered on and do not fresh the page during upgrade. The device will be rebooted automatically later.

Current Version ReyeeOS [redacted]

New Version ReyeeOS [redacted]

Description [redacted]

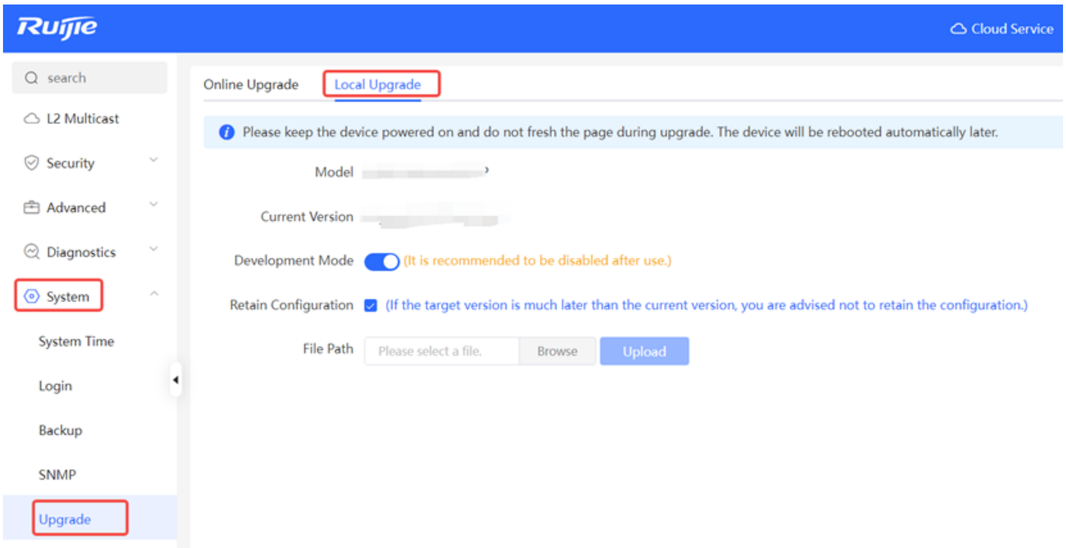
Tips 1. If your device cannot access the Internet, please click Download File.

2. Choose Local Upgrade to upload the file for local upgrade.

12.9.2 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.



Please keep the device powered on and do not fresh the page during upgrade. The device will be rebooted automatically later.

Model [redacted]

Current Version [redacted]

Development Mode (It is recommended to be disabled after use.)

Retain Configuration ☑ (If the target version is much later than the current version, you are advised not to retain the configuration.)

File Path Please select a file.

12.10 Cloud Service

12.10.1 Overview

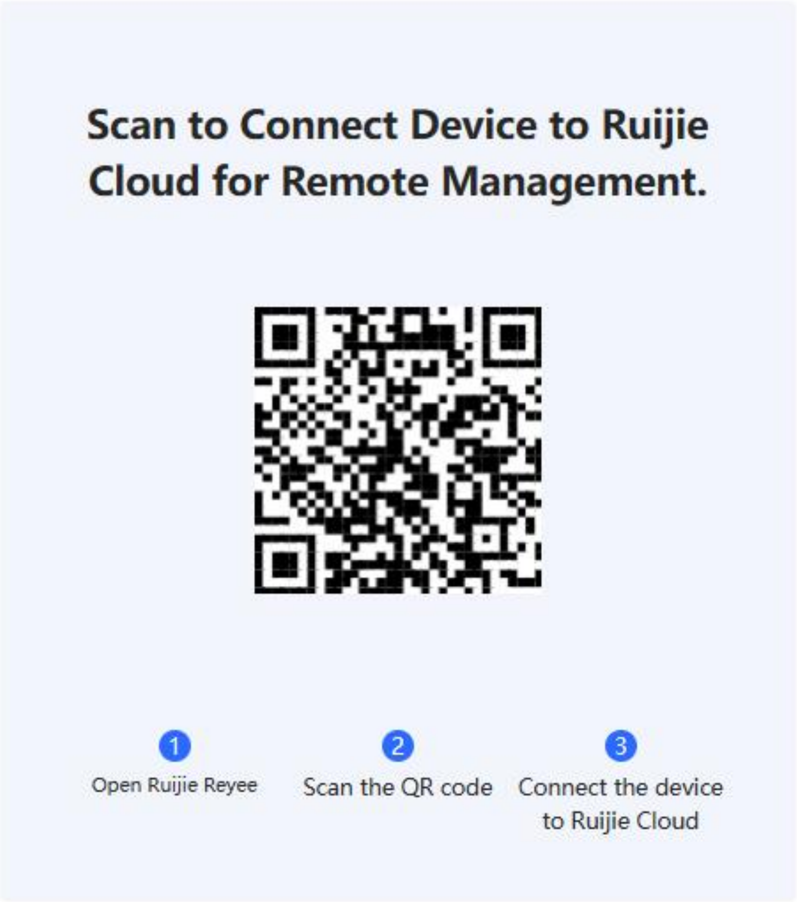
The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently mange networks through Ruijie Cloud or the Ruijie Reyee app.

12.10.2 Configuration Steps

Choose **One-Device** > **Config** > **System** > **Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.



Scan to Connect Device to Ruijie Cloud for Remote Management.

1 Open Ruijie Reyee

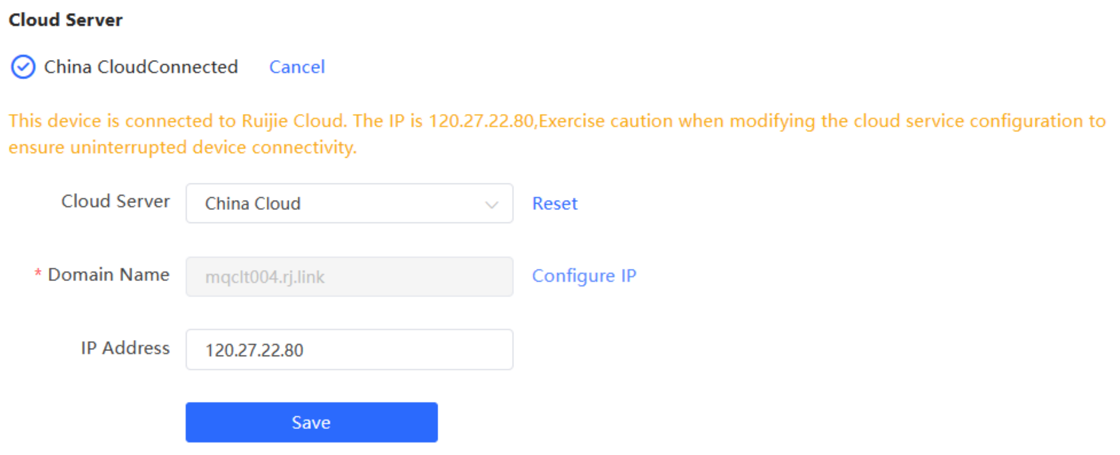
2 Scan the QR code

3 Connect the device to Ruijie Cloud

Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.



Cloud Server

China CloudConnected Cancel

This device is connected to Ruijie Cloud. The IP is 120.27.22.80,Exercise caution when modifying the cloud service configuration to ensure uninterrupted device connectivity.

Cloud Server: China Cloud — Reset

* Domain Name: mqclt004.rj.link — Configure IP

IP Address: 120.27.22.80

To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate.

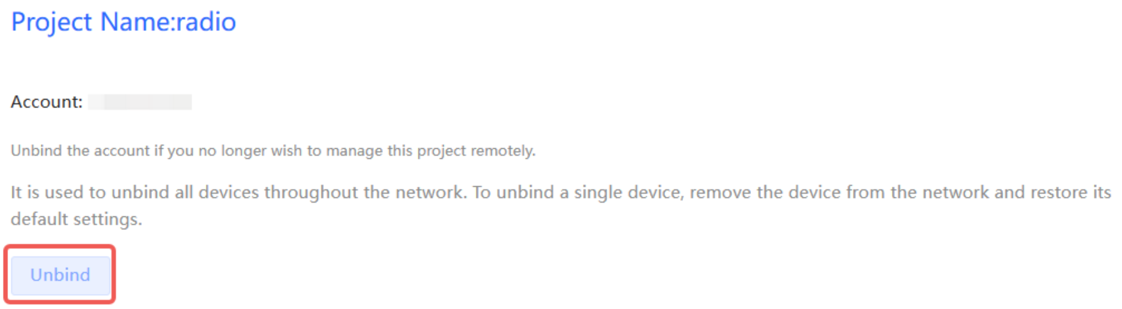
Table 12-12 Cloud Server Description

Parameter	Description
Cloud Server	Geographic location of the cloud server, including China Cloud, Asia Cloud, Europe Cloud, America Cloud, and Other.
Domain Name	Domain name of the cloud server.
IP Address	IP address of the cloud server.

12.10.3 Unbinding Cloud Service

Choose **One-Device** > **Config** > **System** > **Cloud Service**

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.



Project Name:radio

Account:

Unbind the account if you no longer wish to manage this project remotely.

It is used to unbind all devices throughout the network. To unbind a single device, remove the device from the network and restore its default settings.