Ruijie Reyee RG-NBS Series Switches

ReyeeOS 1.230

Web-based Configuration Guide

Document Version: V1.1
Date: August 15, 2023
Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

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

Trademarks including  ,  are owned by Ruijie Networks.

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

Disclaimer

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com

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.

1 Login

1.1 Configuration Environment Requirements

1.1.1 PC

- 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.

1.2 Logging in to the Web Page

1.2.1 Connecting to the Device

Use a network cable to connect the switch port to the network 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 through the switch. For example, set the IP address of the PC to 10.44.77.100.

Table 1-1 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.

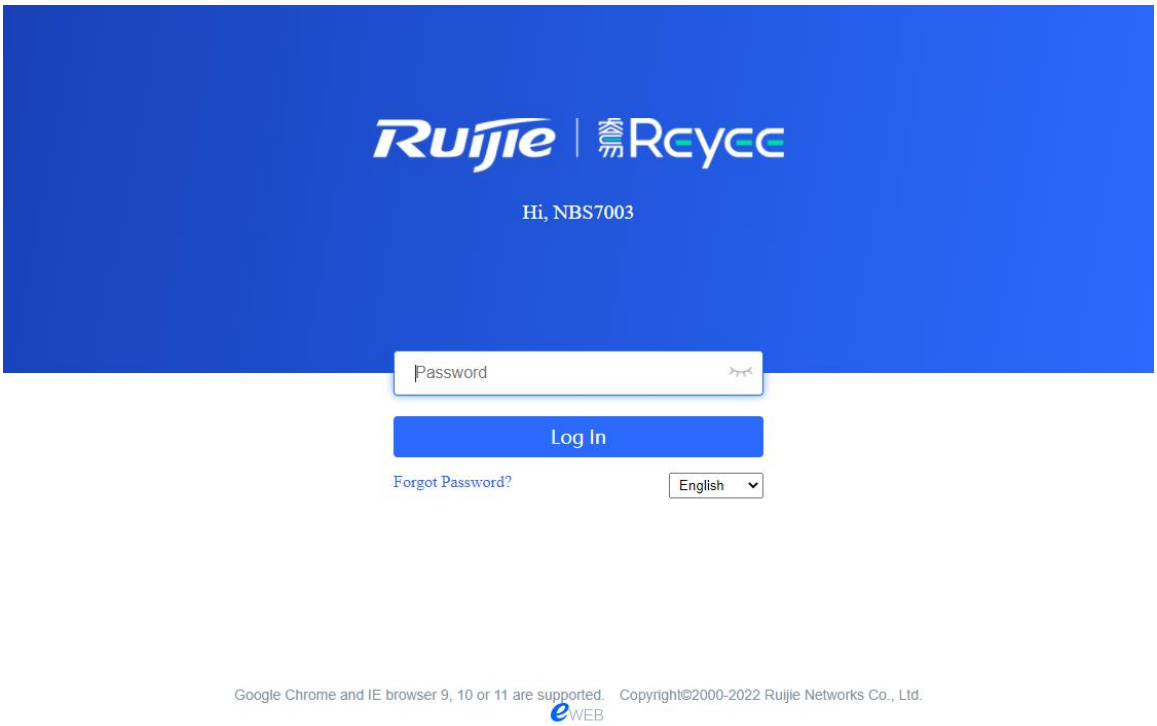
1.2.2 Logging in to the Web Page

(1) Enter the IP address (10.44.77.254 by default) of the device in the address bar of the browser to open 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 open the homepage of the web management system.



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 5s when the device is connected to the 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.

1.2.3 Frequently-Used Controls on the Web Page

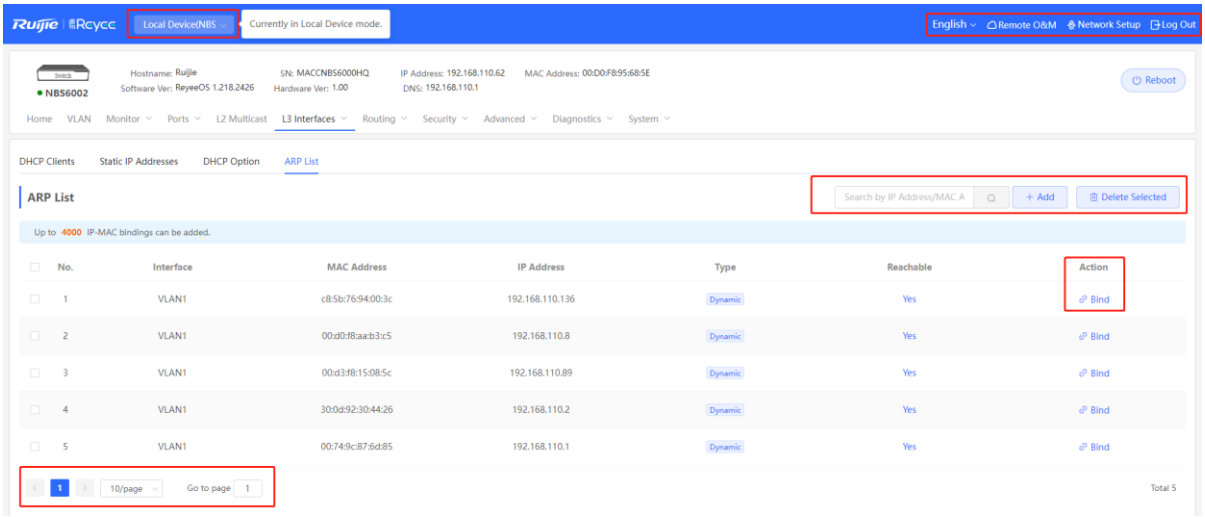
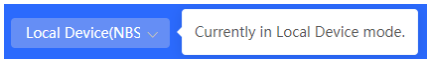
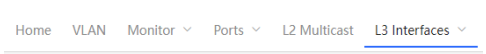
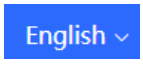
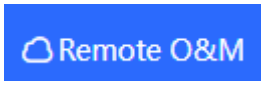
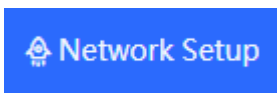
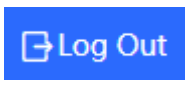
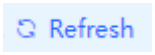
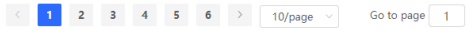


Table 1-2 Frequently-Used Controls on the Web Page

Control	Description
	**Local Device**: Allows you to configure all functions of the local device. **Network**: Allows you to configure common functions of all wired and wireless Reyee products in batches in an ad hoc network.
	The navigation bar is arranged horizontally on the top when the device acts as a slave device, and vertically on the left when the device acts as a master device.
	Click it to change the language.
	Click it to log in to the MACC for remote O&M through the URL or by scanning the QR code.
	Click it to access the network setup wizard.
	Click it to log out of the web management system.
	Click **Add** or **Batch Add** to add one or more table entries in the dialog box that appears. After adding the table entries,

	you can view the added table entries on this page.
	Click it to delete the selected table entries in batches.
	Quickly locate the table entry you want to find through the drop-down list or by entering a keyword.
	Click them to edit, delete, or bind a table entry.
	If the toggle switch is displayed in gray and the button is on the left, the related function is disabled. If the toggle switch is displayed in blue and the button is on the right, the related function is enabled.
	Update data on the current page.
	Set the number of table entries displayed on a page. Click a page number or specify the page number to go to the corresponding page.

1.3 Quick Setup

1.3.1 Configuration Preparations

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

1.3.2 Procedure

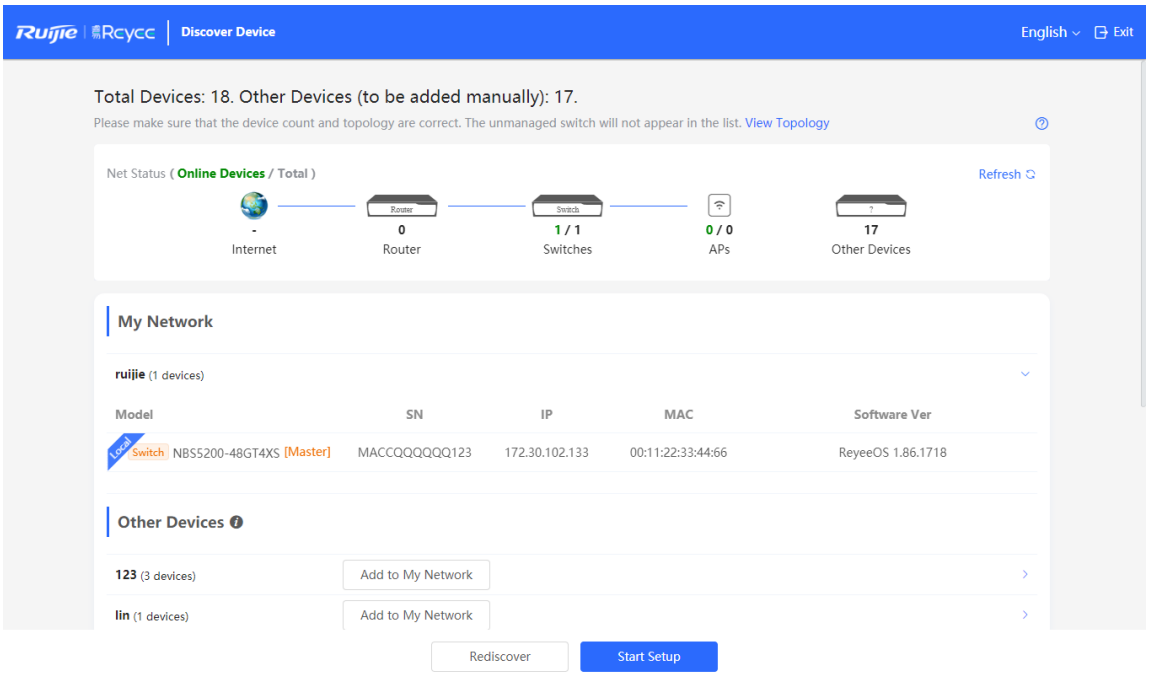
1. Adding Device to Network

By default, users can perform batch settings and centralized management of all devices in the network. Therefore, before starting configuration, you need to check and confirm the number of online devices and network status in 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 in the network that are not added to the current network, you can click **Add to My Network** and enter the management password of the added device to manually add the corresponding device to the network where the device is located, and then start the network-wide configuration.



2. Creating a Web Project

Click **Start Setup** to set the networking modes and management password of the device.

(1) **Network Name:** Identify the network where the device is located.

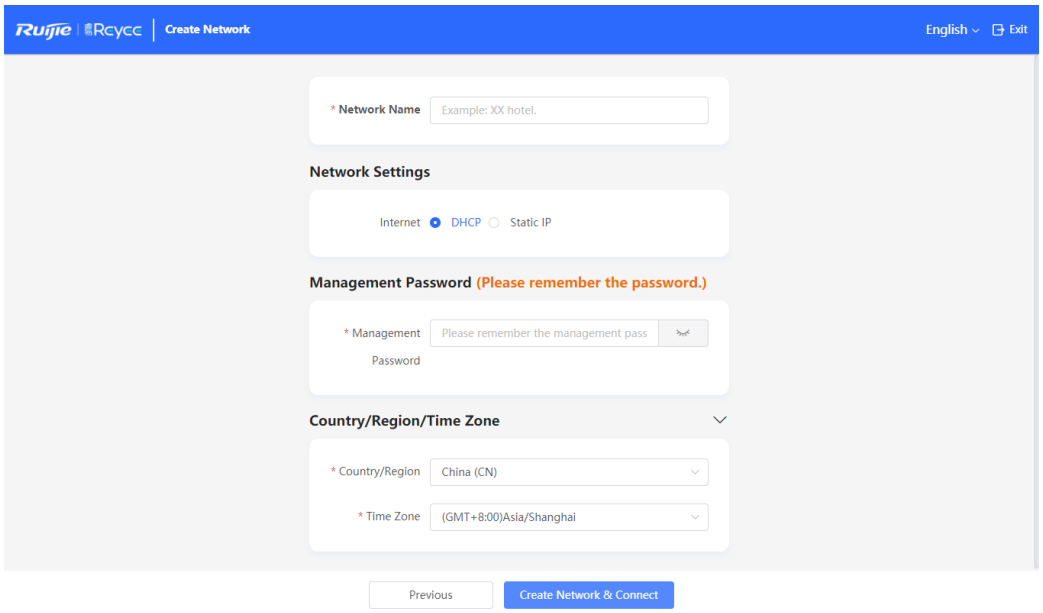
(2) **Internet:** Select the networking mode.

- **DHCP**: An IP address is assigned to the device by the uplink DHCP server. By default, the device detects whether the IP address can be dynamically obtained. If the IP address is obtained successfully, there is no need to manually set the IP address.
- **Static IP**: The user manually enter a specified IP address, subnet mask, gateway IP address, and DNS address.

(3) **Management Password:** Set the password for logging in to the management page.

(4) **Country/Region**: Select the country or region where the device is located.

(5) **Time Zone:** Set the system time. The network time server is enabled to provide time services by default. Please select your actual time zone.



Click **Create Network & Connect** to deliver related configuration for initialization and detect the network. After completing the quick setup, the new device is connected to the Internet, and you can continue to bind the device to the cloud account for remote management. For specific operations, please refer to the instructions on the page to log in to the Noc Cloud platform for configuration.

Note

- Click **Exit** in the upper right corner and follow prompts to perform operations. Then, the device can skip quick setup to go to the Eweb management system. To configure again after exiting or completing the quick configuration, click the sign in the navigation bar at the top of the web page.
- After changing the management password, you need to re-visit the device management address and use the new password to log in to the device.

1.3.3 Procedure for Configuring Hot Standby (VCS)

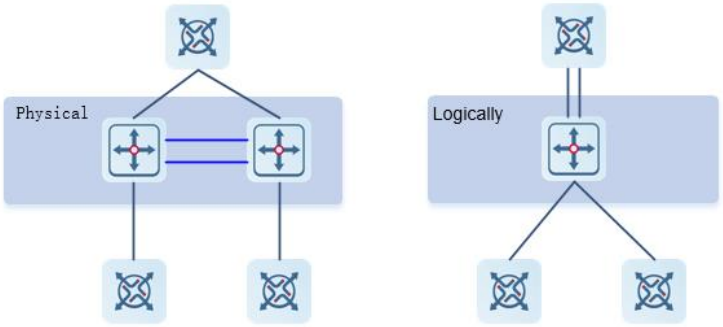
The VCS (Virtual Chassis System) is a feature that provides virtualization and clustering capabilities for switches. VCS technology allows multiple physical switches to form a logically unified device, creating a virtual switch stack. This stack is treated as a single entity with shared management and data planes.

Hot standby can improve data forwarding reliability when an NBS switch is used as the core switch. By stacking two switches and automatically switching to the standby switch when the active switch fails, hot standby ensures uninterrupted data forwarding in the event of a single point of failure.

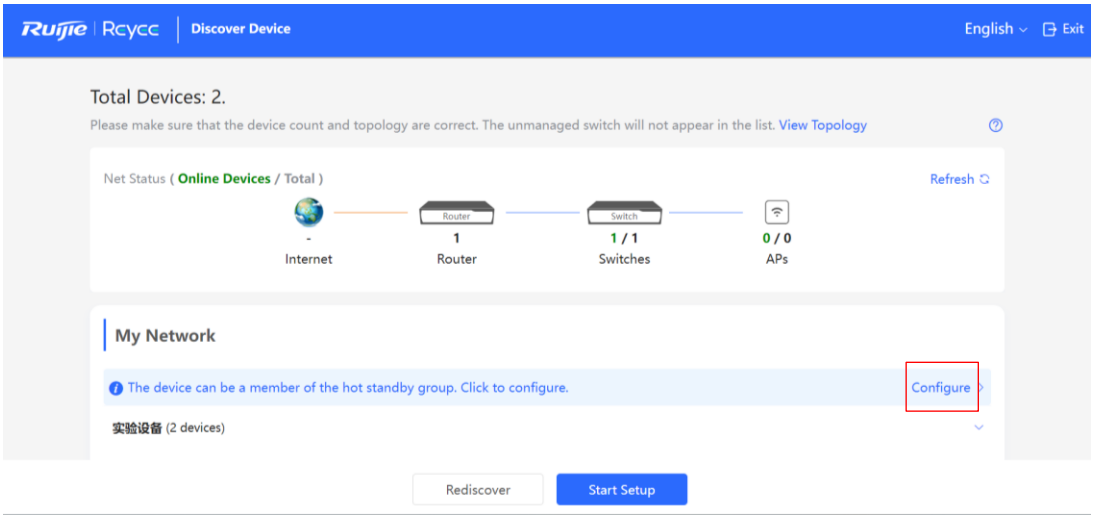
Caution

- Hot standby is supported only on NBS7006 and NBS7003 series switches.
- Only two switches are supported to form a hot standby group.
- When multiple switches are configured, select 10GE interfaces as hot standby interfaces to connect the member switches.

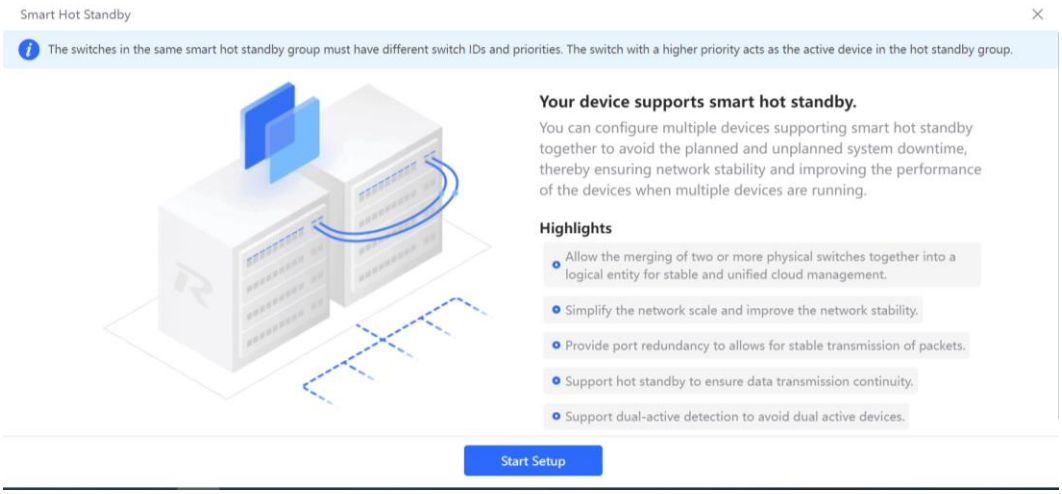
Stacking: refers to physically connecting multiple switches with stack cables, allowing them to operate as a single logical unit for data forwarding.



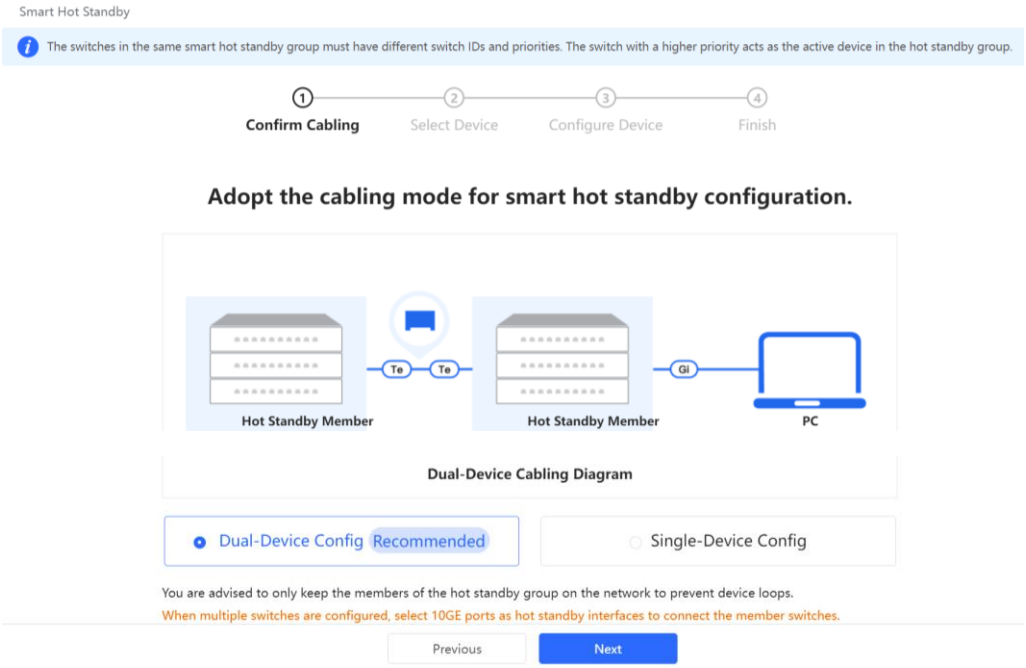
(1) Enter the default IP address 10.44.77.200 in the address bar of your browser to go to the web management interface of the NBS switch. Click the **Hot Standby** tab (or click **Configure** in the red box below if the switch is not yet configured).



(2) Click **Start Setup**.



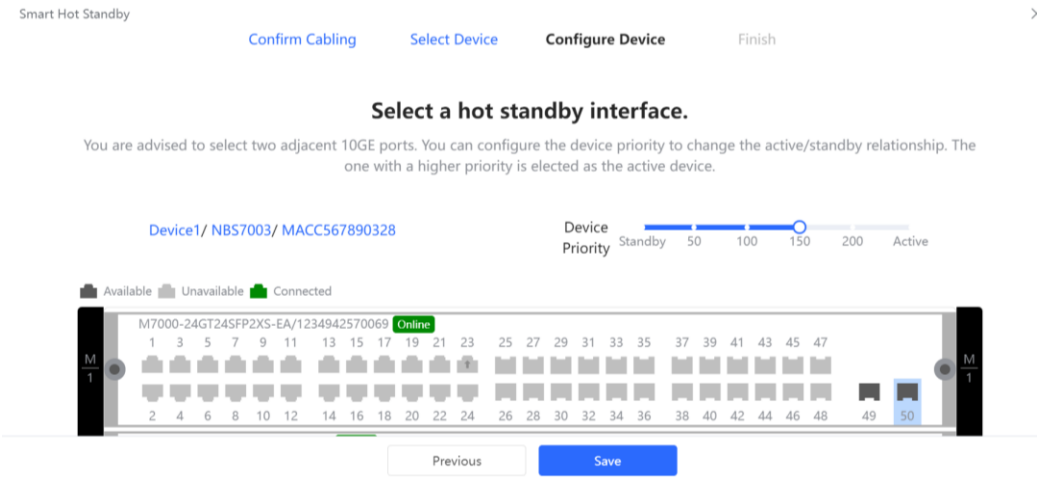
(3) Connect both switches using a network cable on their 10GE interfaces. Then, choose **Dual-Device Config**, and click **Next**.



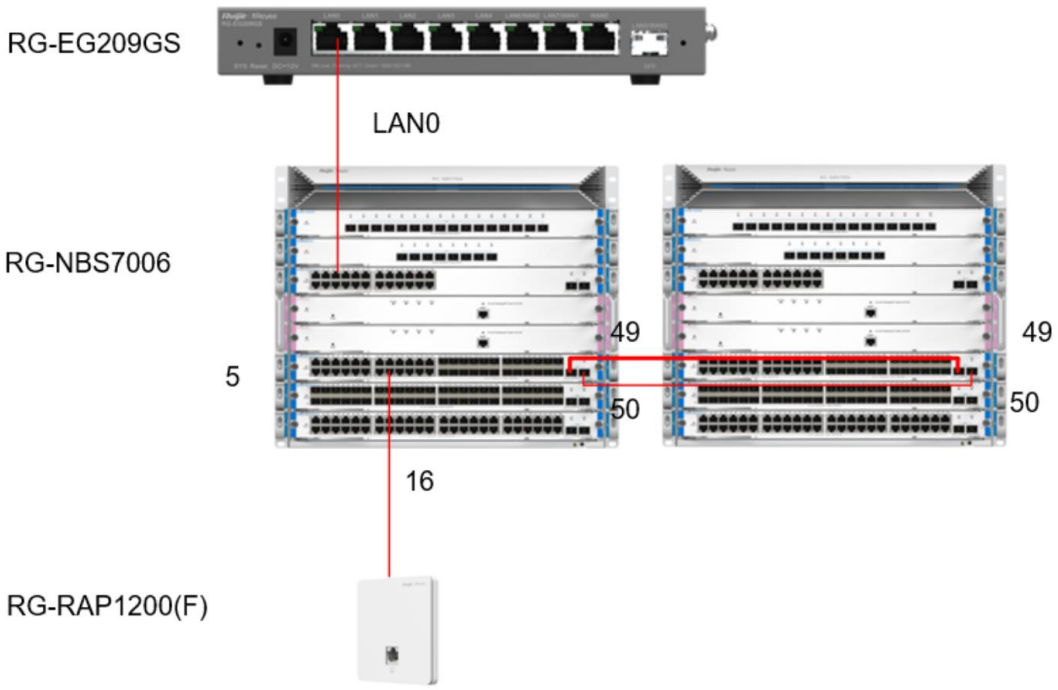
(4) Select the active switch and click **Next**.

(5) Select the standby switch.

(6) Select the hot standby interfaces. You are advised to select two adjacent interfaces on a switch, and can select up to four interfaces on each device for hot standby. These hot standby interfaces must be 10GE interfaces. By default, the active switch has a priority of 200, while the standby switch has a priority of 100. If the priority is changed, a switch with a higher priority will become the active switch.



(7) Then, click **Next**. Use a 10GE cable to connect the hot standby interfaces that you have selected. (The following figure shows an example of connecting Interface 49 of Device 1 to Interface 49 of Device 2.)



(8) After the cables are connected, proceed as prompted, and wait for the device to reboot successfully.

Caution

To delete the hot standby configuration, ensure that the network cable connecting the hot standby interfaces is disconnected. Failure to do so may result in a loop that can cause network disconnection.

1.4 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 in the network and discover other devices in 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 in 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 page has two configuration modes: the network mode and the local device mode. For more information, see Switching the Management Mode.

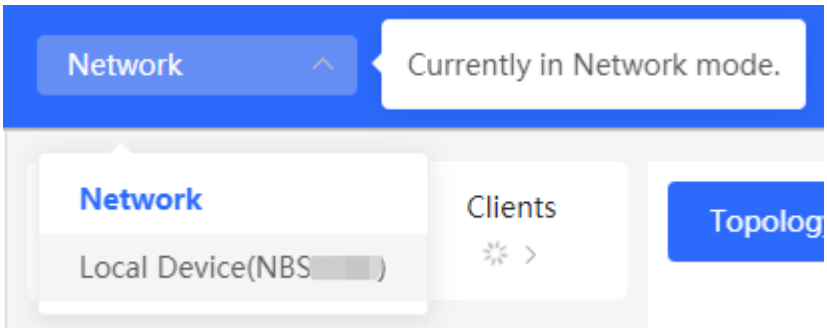
Standalone mode: If the self-organizing network discovery function is disabled, the device will not be discovered in the network. After logging in to the Web page, you can configure and manage only the currently logged in

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.

1.5 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

In self-organizing network mode, the Web page has the network mode and the local device mode. Click the **Currently in Network** mode in the navigation bar and select the desired mode from the drop-down list box.



- The network mode: Display the management information of all devices in the network and configure all devices in the current network from the network-wide perspective. As shown in;
- The local device mode: Only configure the device that you log in to. As shown in.

Figure 1-1 The Web Page in Standalone Mode

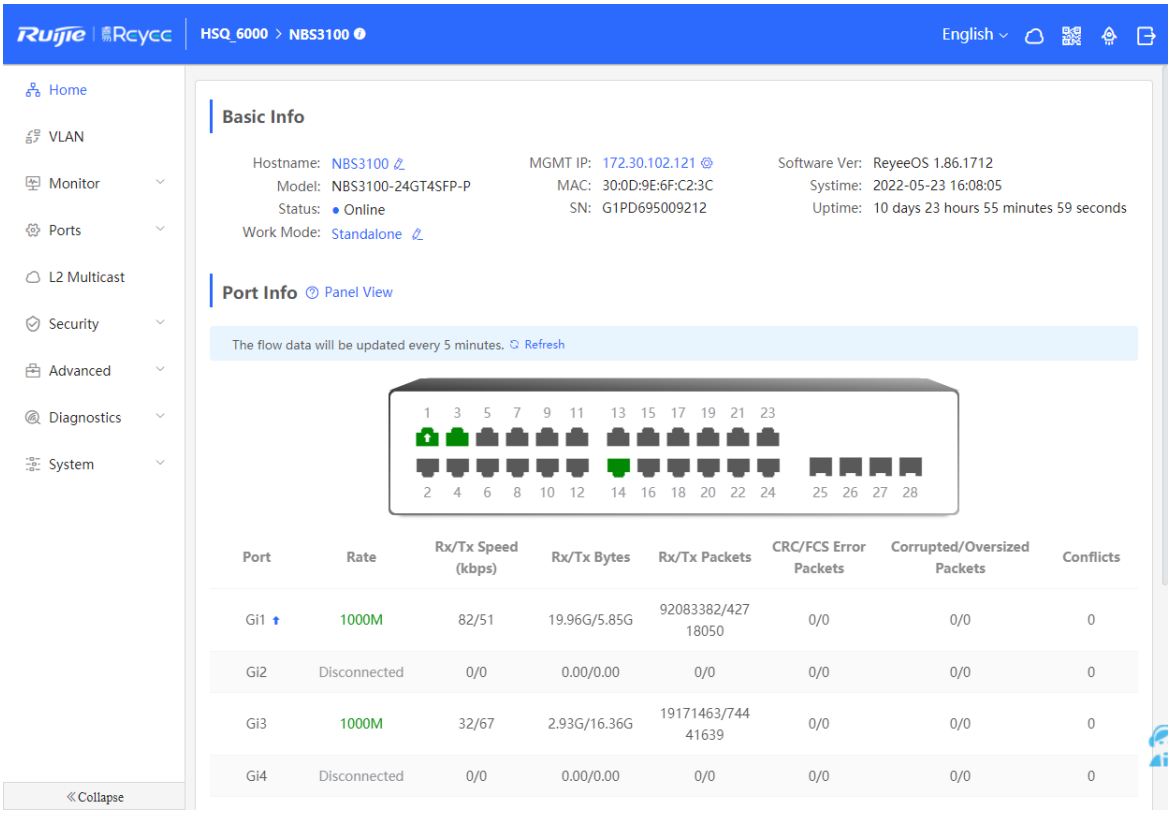


Figure 1-2 The Web Page in Network Mode in Self-Organizing Mode

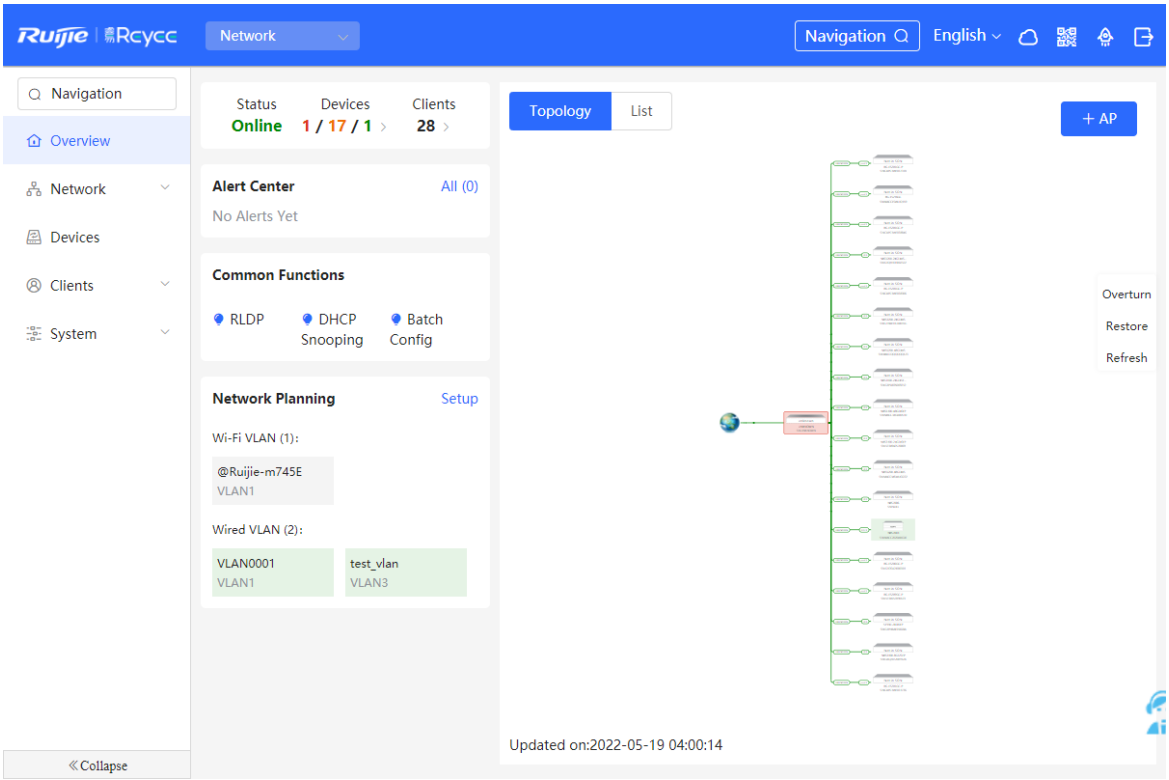
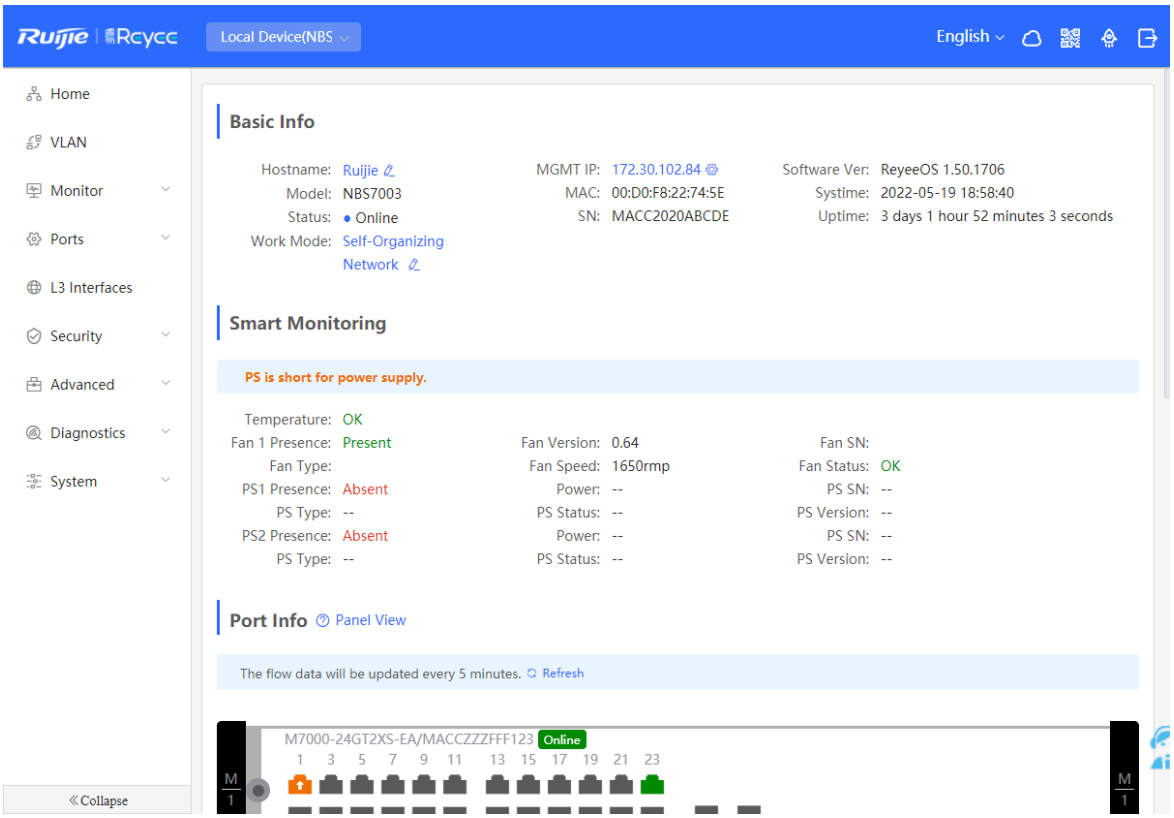


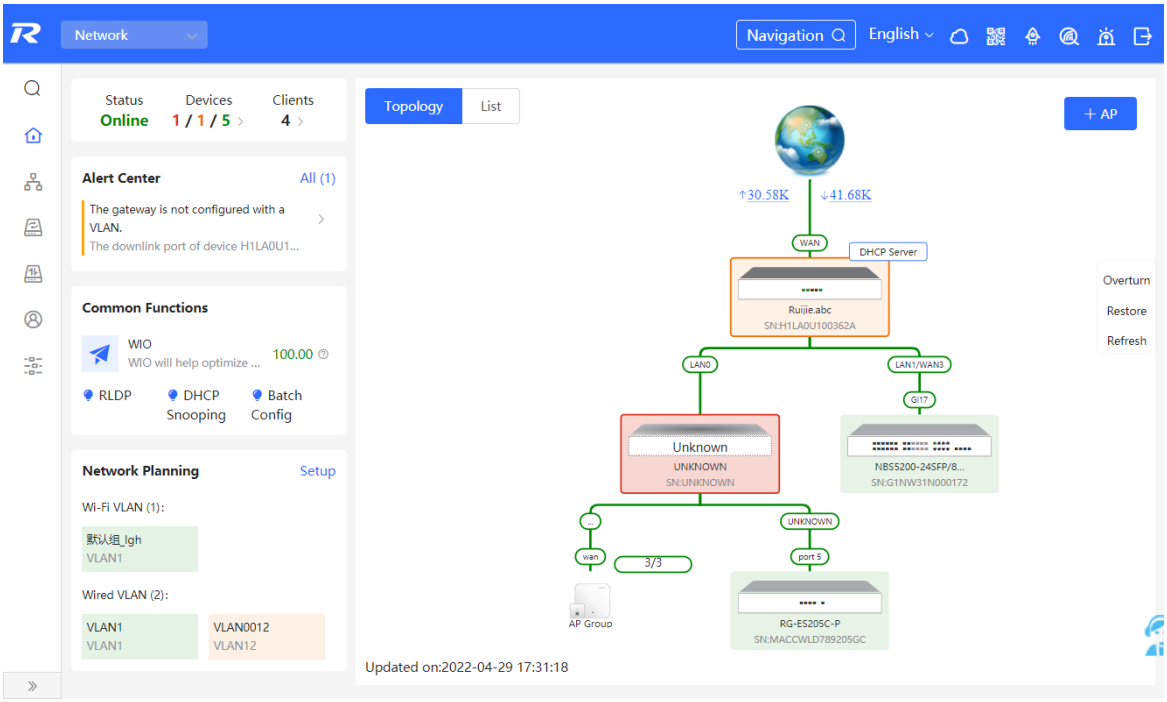
Figure 1-3 The Web Page in Local Device Mode in Self-Organizing Mode



2 Network management

2.1 Overviewing Network Information

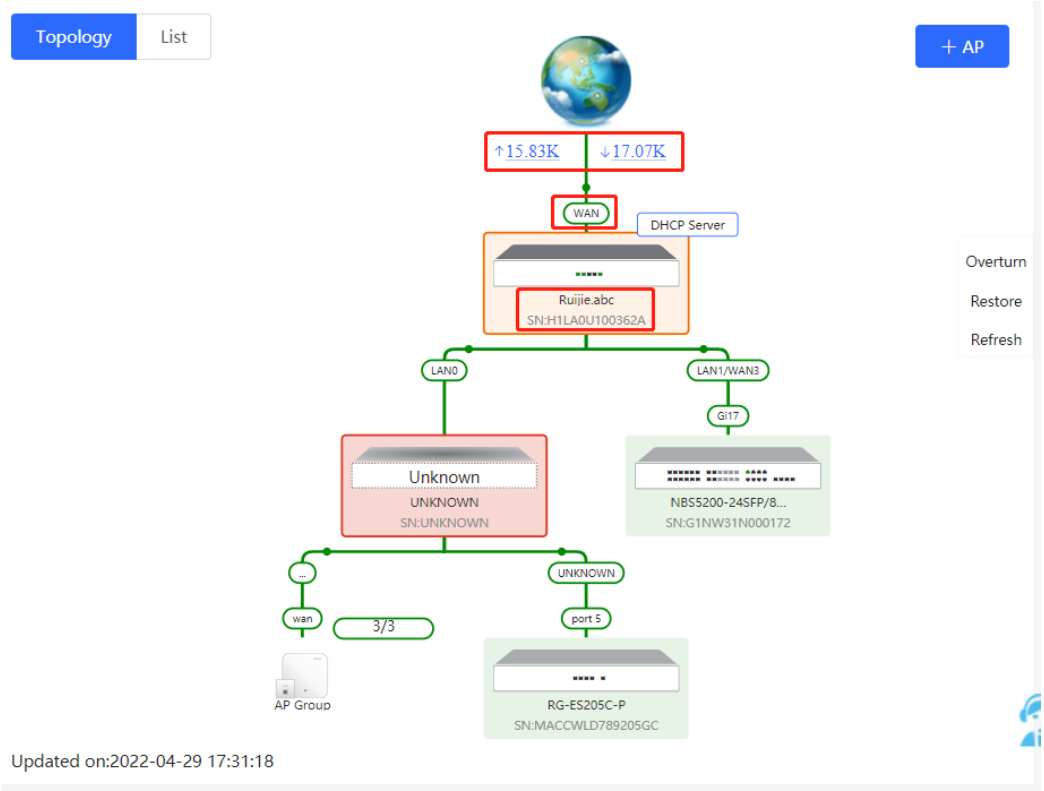
In network mode, the **Overview** page displays the current network topology, uplink and downlink real-time traffic, network connection status, and number of users and provides short-cut entries for configuring the network and devices. Users can monitor and manage the network status of the entire network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



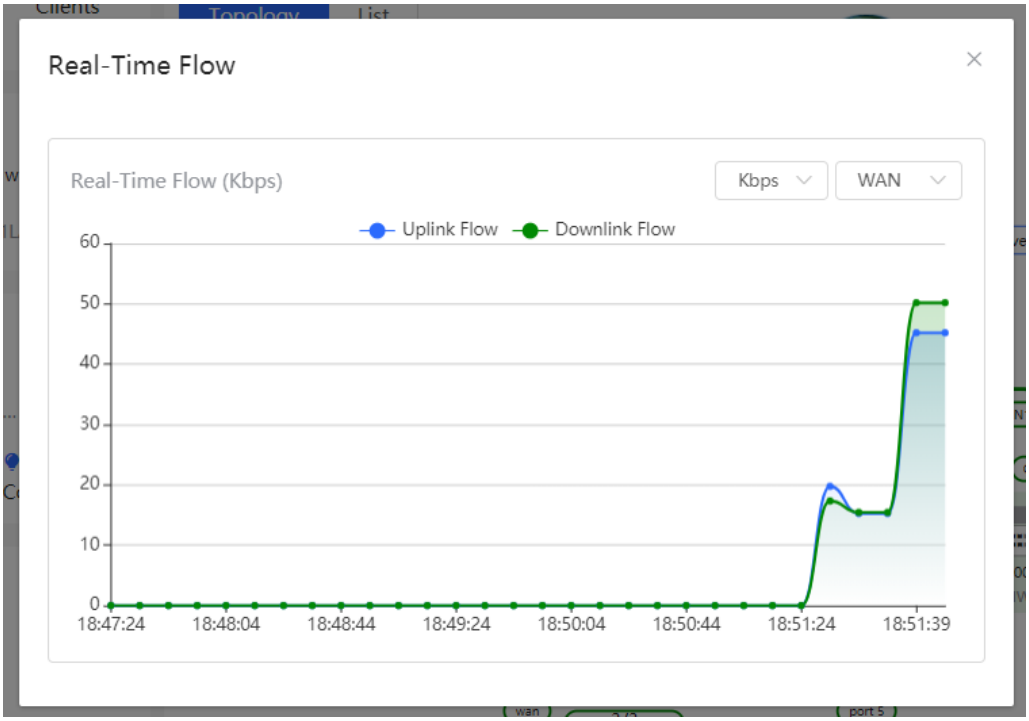
2.2 Viewing Networking Information

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

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

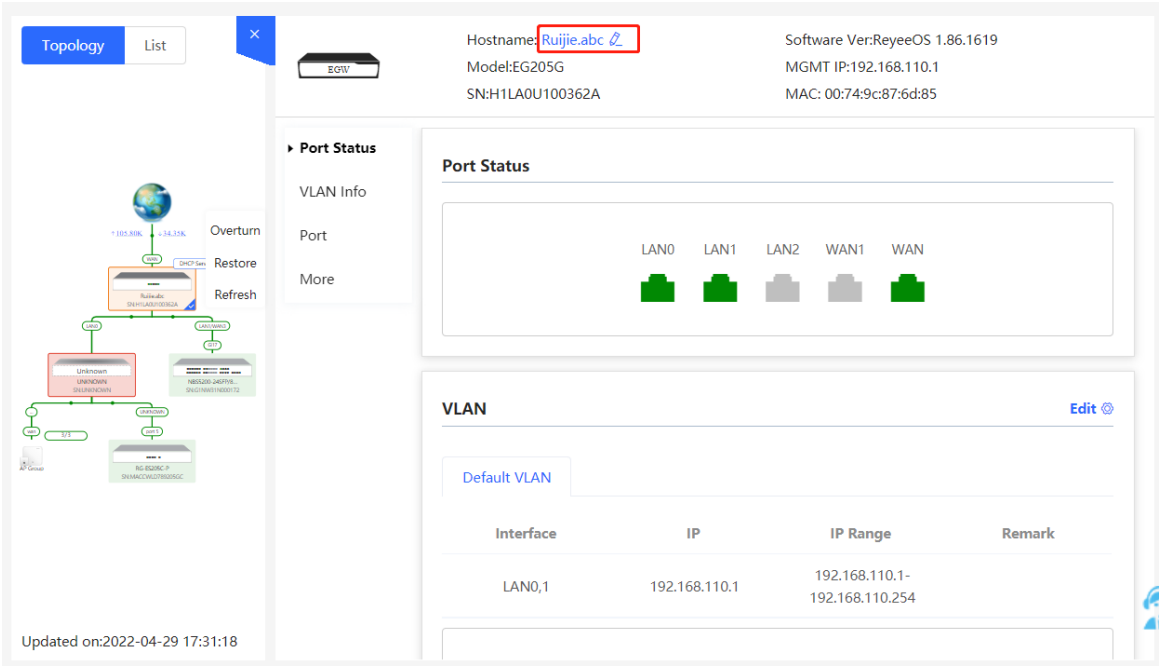


- Click a traffic data item to view the real-time total traffic information.

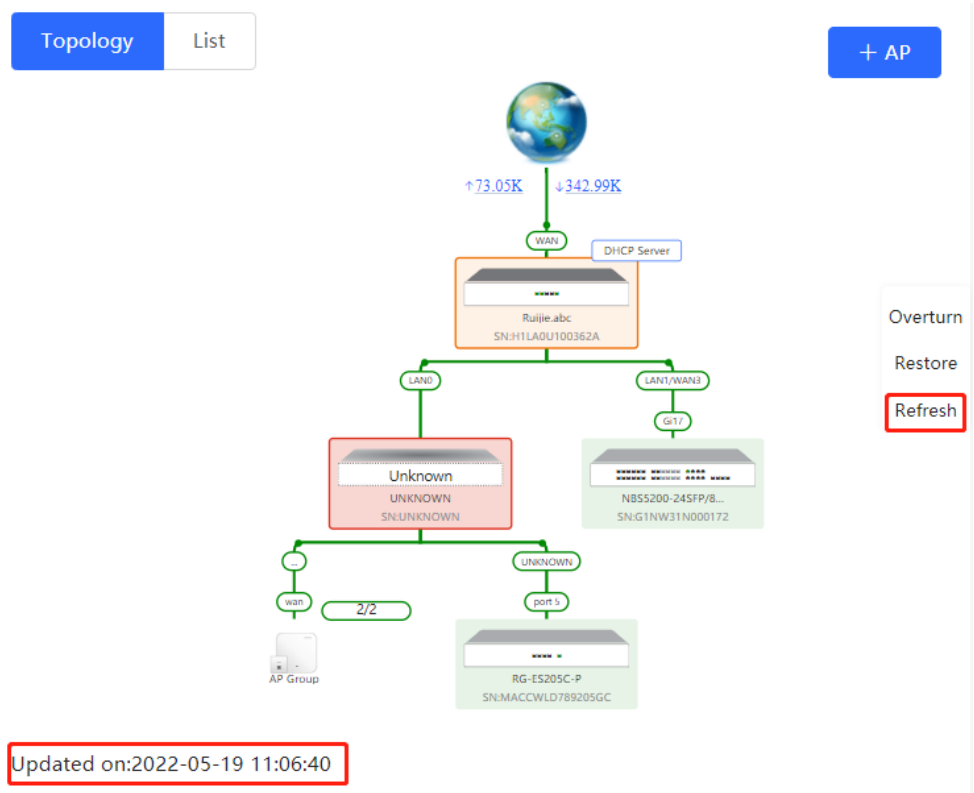


- Click a device in the topology to view the running status and configuration of the device and configure device functions. By default, the product model is used as the device name. Click to modify the device name

so that the description can distinguish devices from one another.



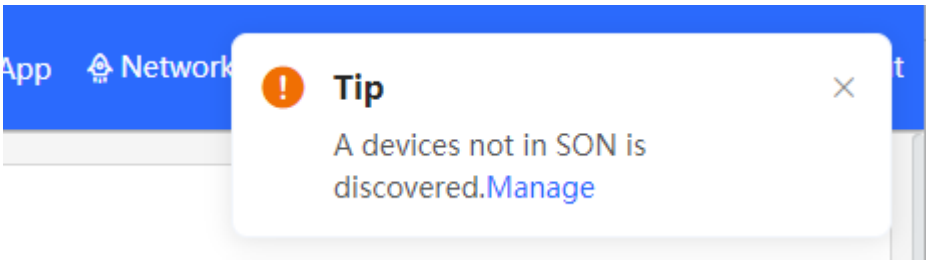
- The update time is displayed in the lower-left corner of the topology view. Click **Refresh** to update the topology to the latest state. It takes some time to update the topology data. Please wait patiently.

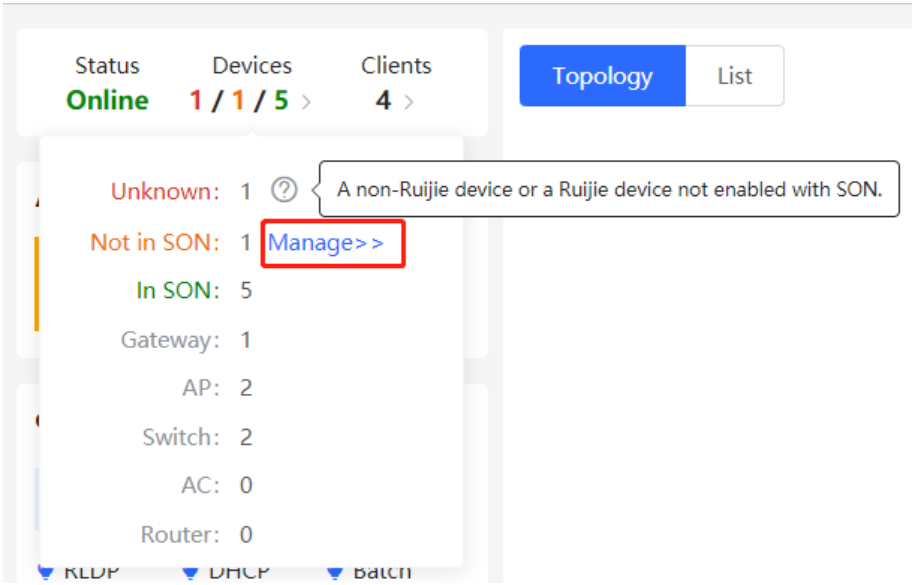


2.3 Adding Networking Devices

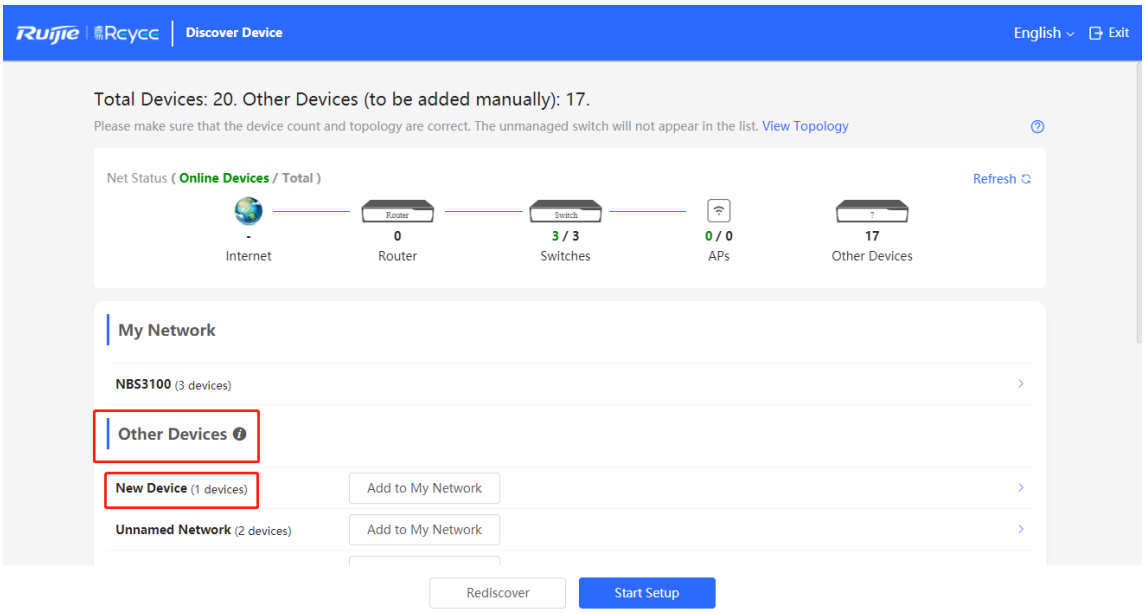
2.3.1 Wired Connection

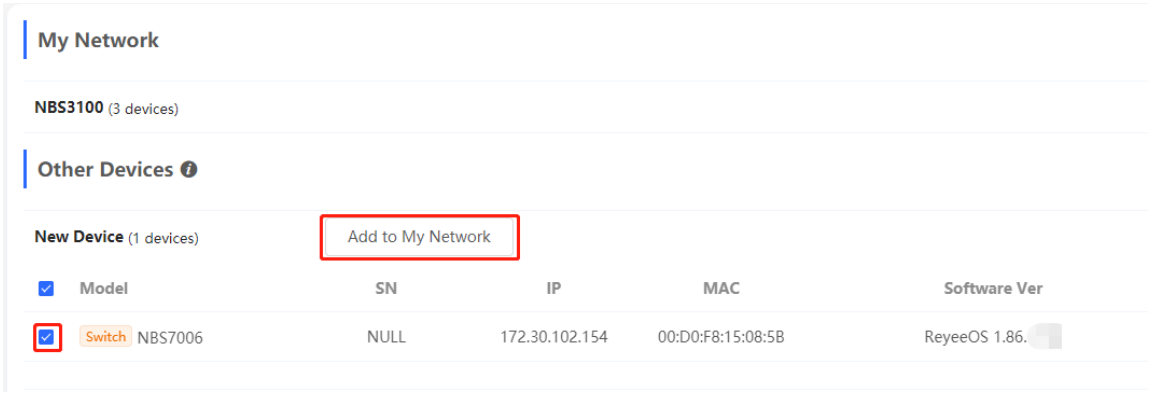
(1) When a new device connects to an existing device on the network, the system displays the message "A device not in SON is discovered." and the number of such devices in orange under "Devices" on the upper-left corner of the [Overview] page. You can click **Manage** to add this device to the current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



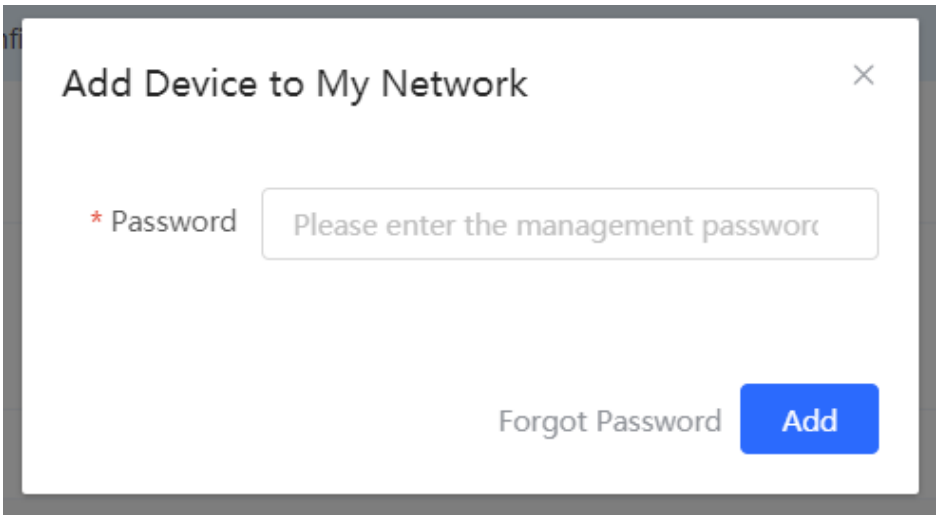


(2) After the system switches to the **Network List** page, click **Other Network**. In the **Other Network** section, select the device to be added to the network and click **Add to My Network**.





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



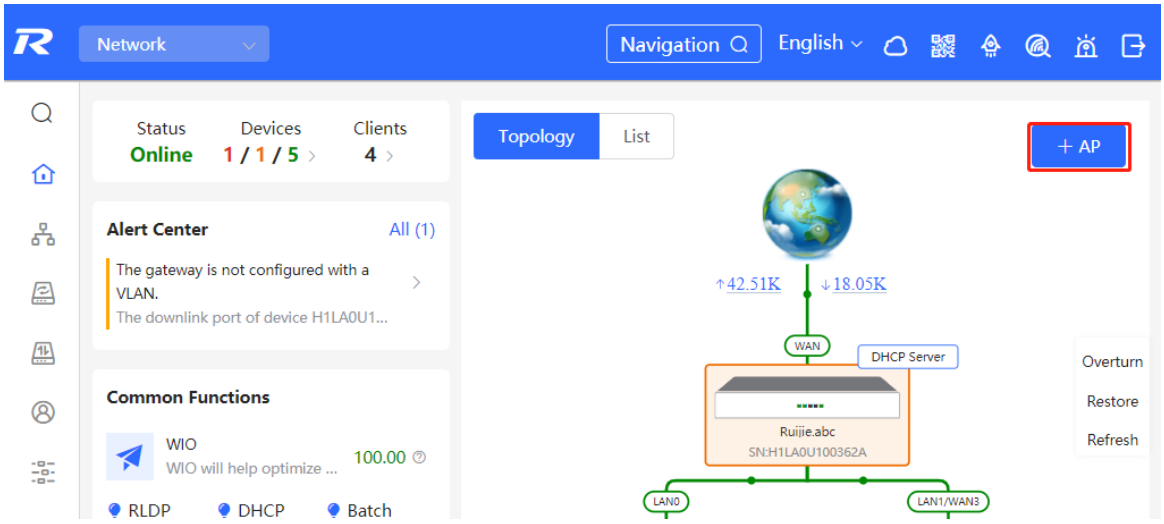
2.3.2 AP Mesh

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

Caution

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

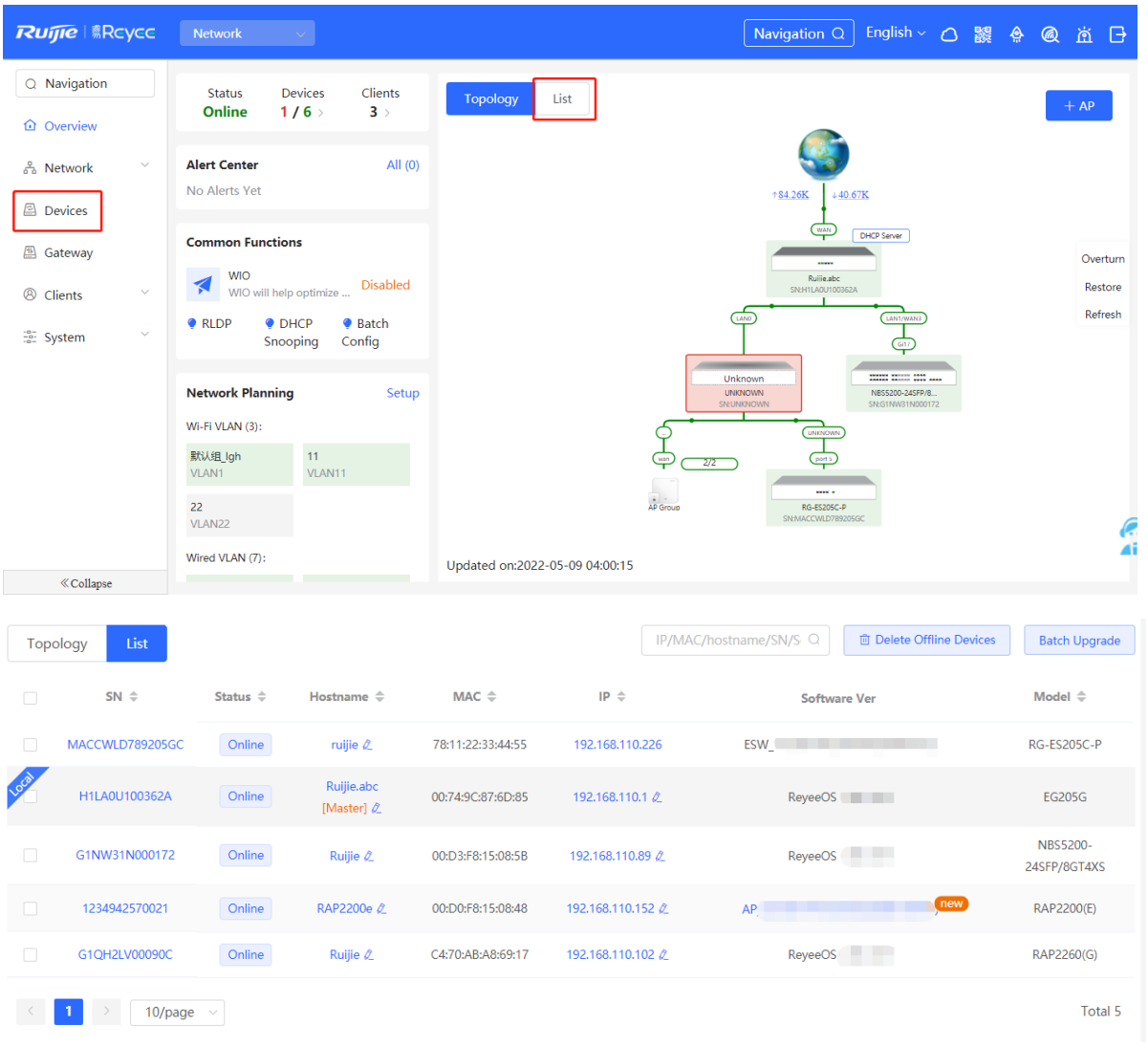
(1) Place the powered new AP near an existing AP, where the new AP can receive Wi-Fi signals from the existing AP. Log in to a device in the network. On the **Overview** page, click **+AP** in the upper-right corner of the topology to scan nearby APs that do not belong to the current network and are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



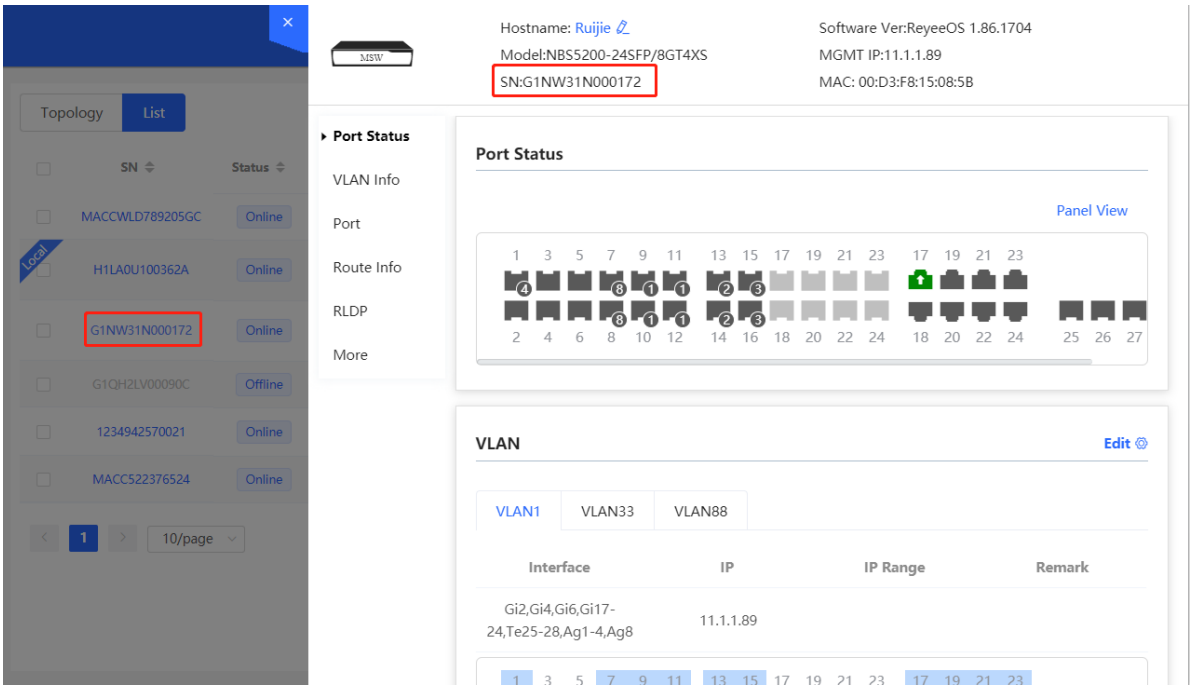
(2) Select the target AP to add it to the current network. You do not need to enter the password if the device to add is new. If the device has a password, enter the management password of the device.

2.4 Managing Networking Devices

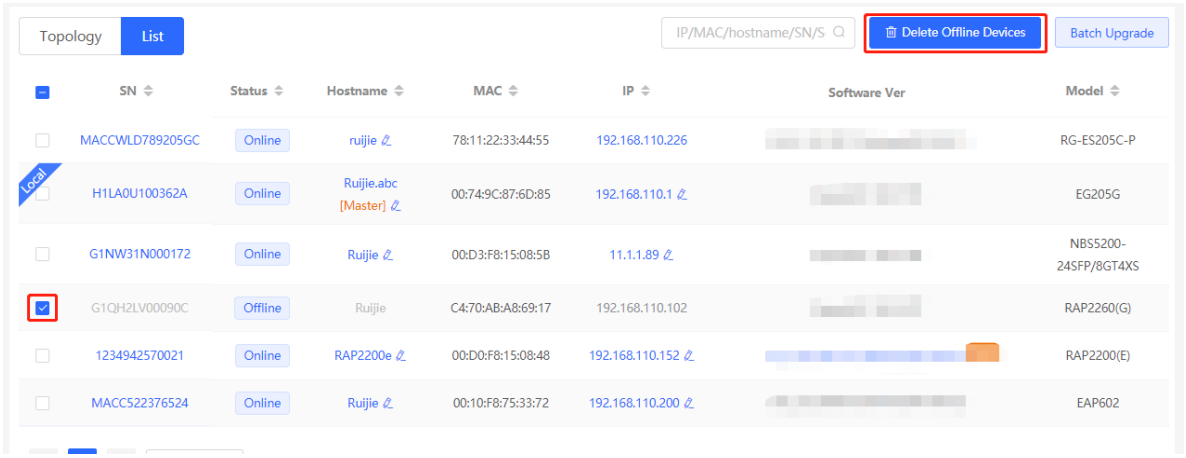
On the **Overview** page, click **List** in the upper-left corner of the topology or click **Devices** in the menu bar to switch to the device list view. Then, you can view all the device information in the current networking. Users only need to log in to one device in the network to configure and manage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



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

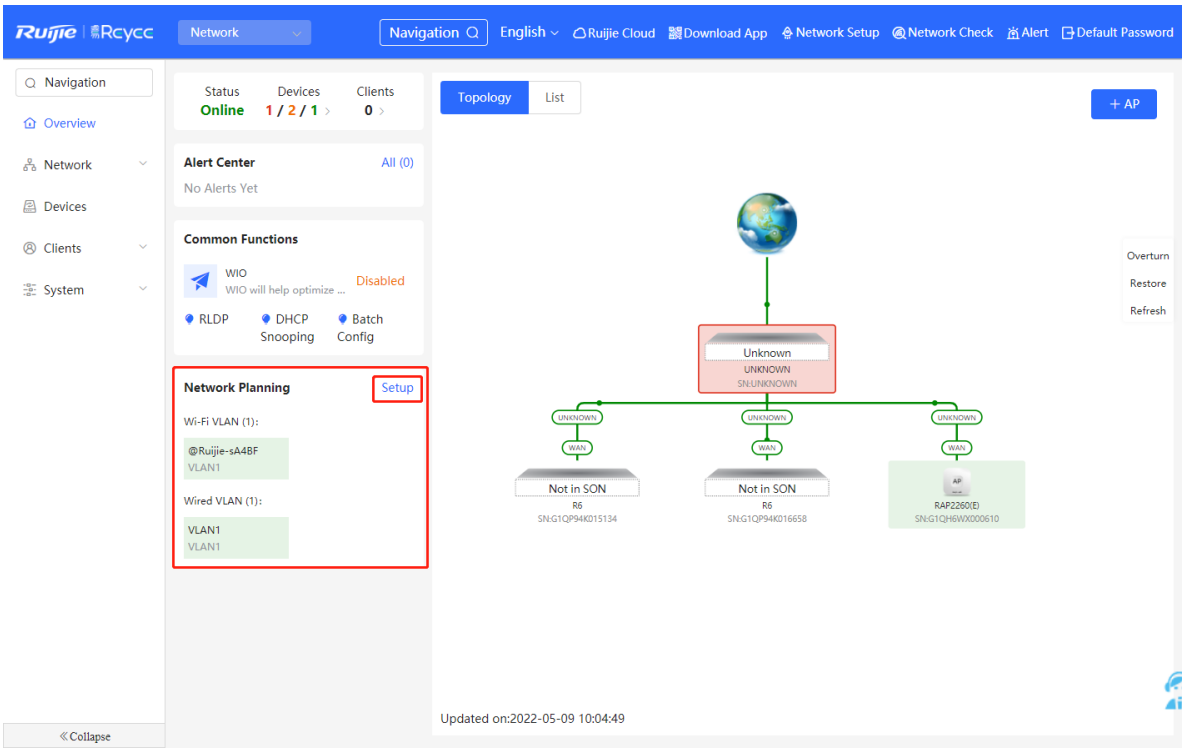


- Check offline devices and click **Delete Offline Devices** to remove them from the list and networking topology.



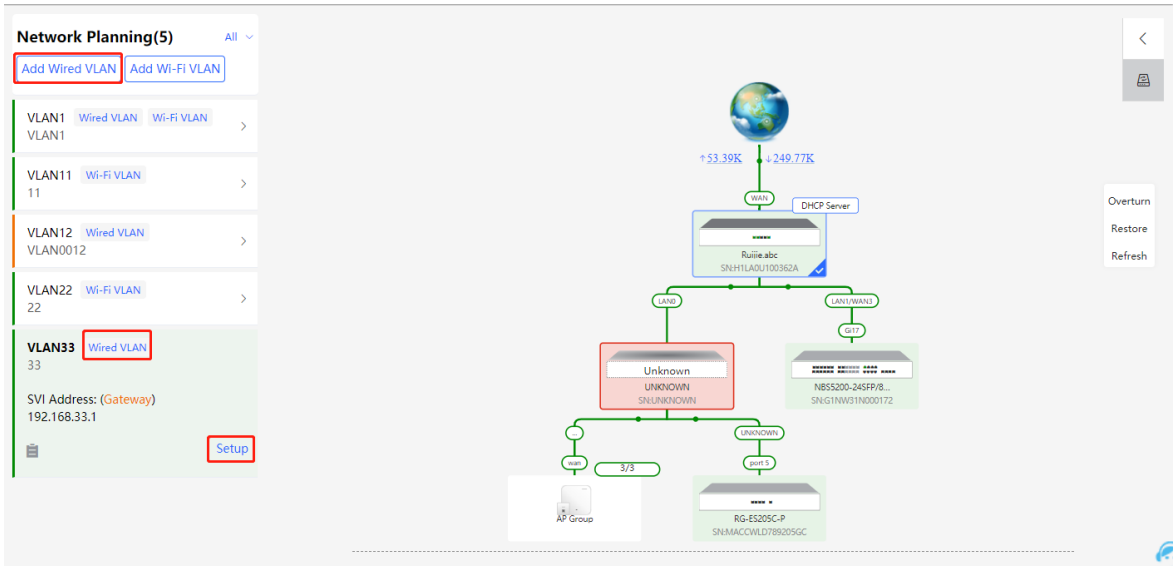
2.5 Configuring the Service Network

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

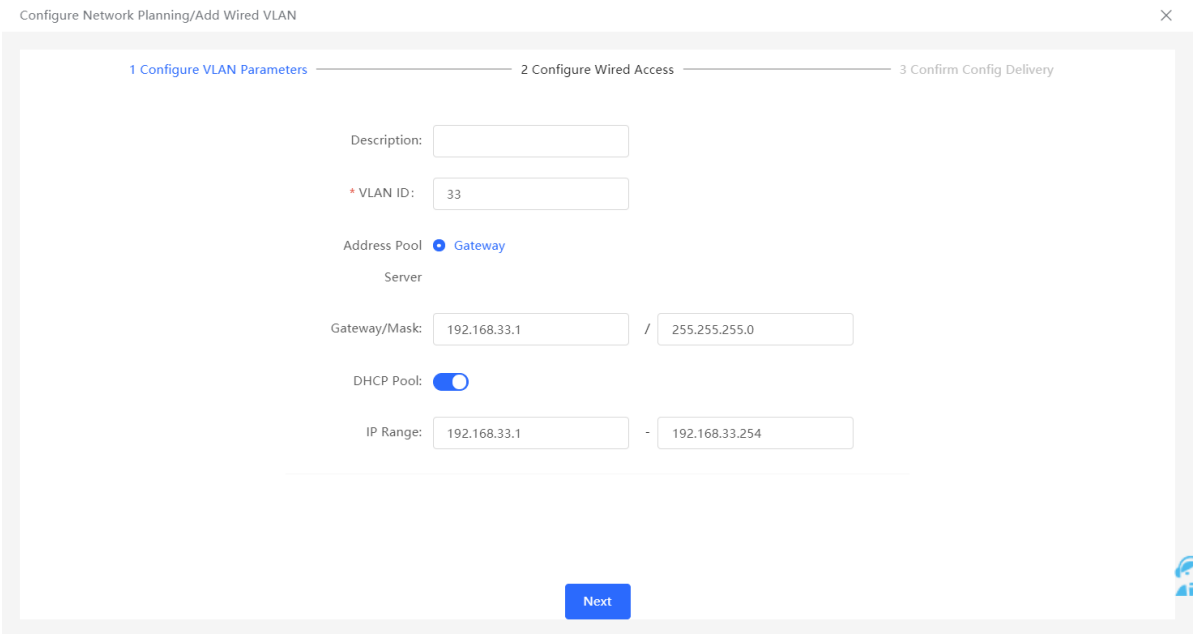


2.5.1 Configuring the Wired Network

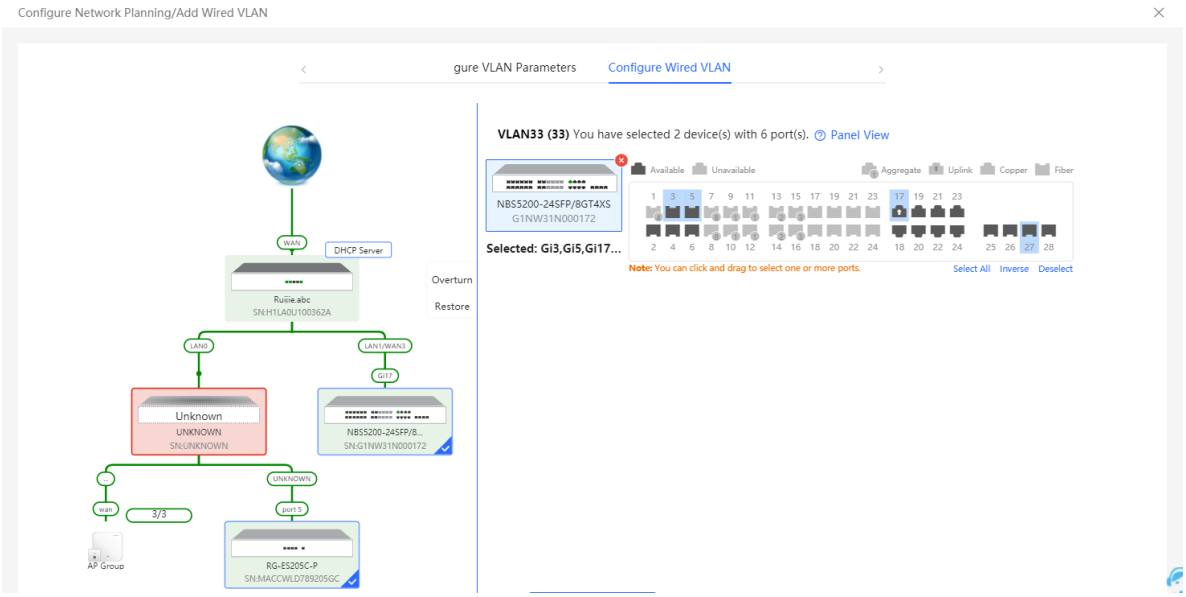
(1) Click **Add Wired VLAN** to add wired network configuration, or select an existing wired VLAN and click **Setup** to modify its configuration.



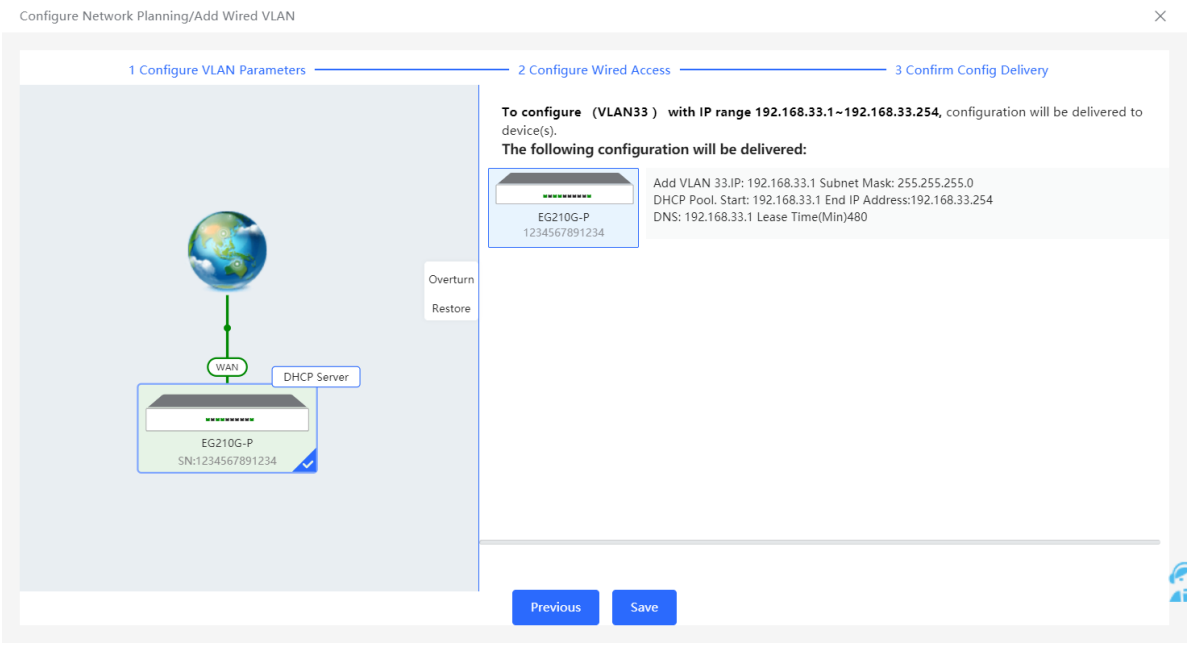
(2) Configure a VLAN for wired access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. A switch or gateway device can be selected as the address pool server. After setting the service parameters, click **Next**.



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

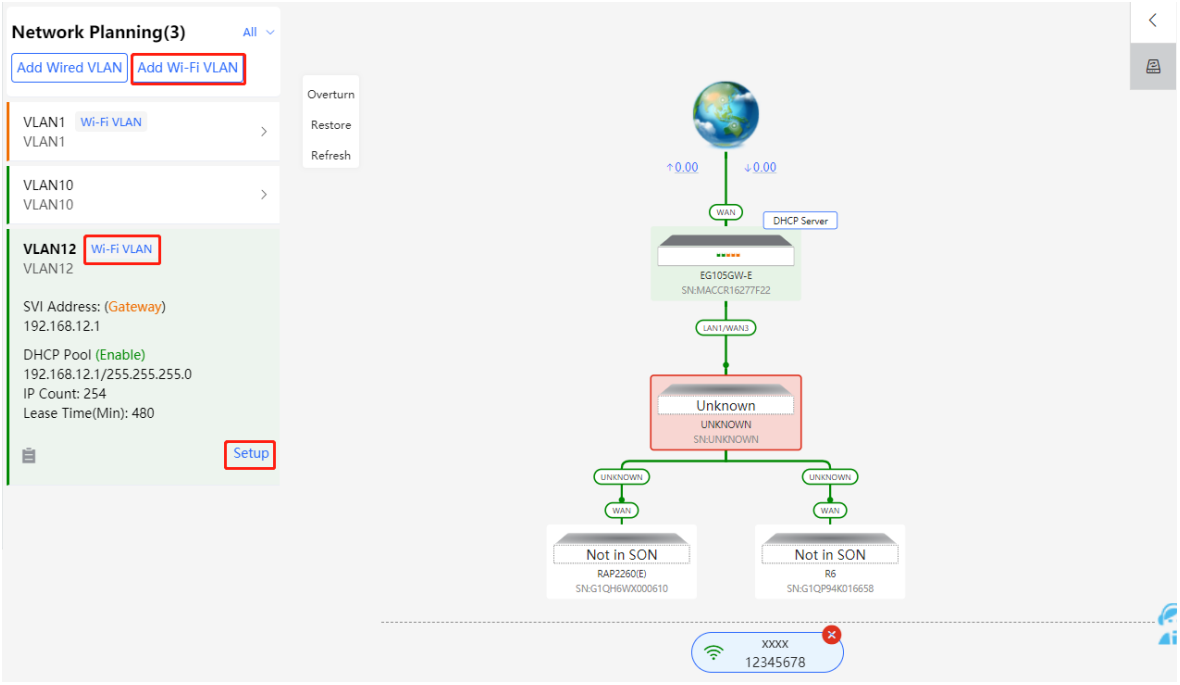


(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.

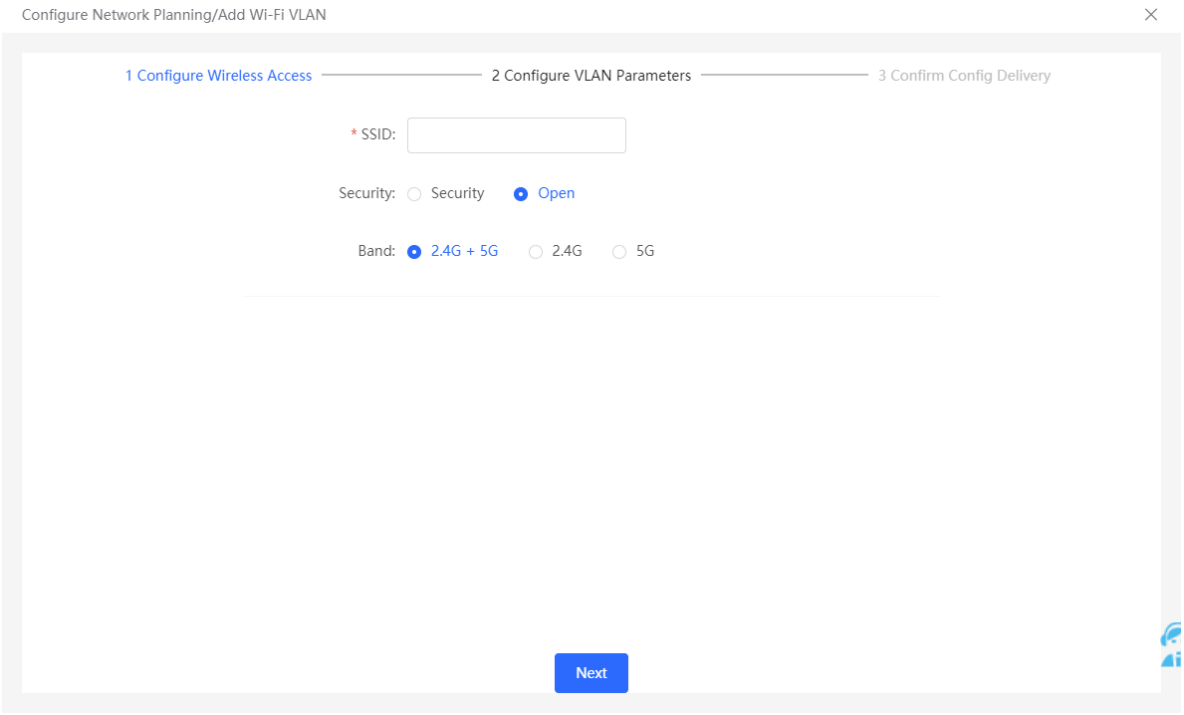


2.5.2 Configuring the Wireless Network

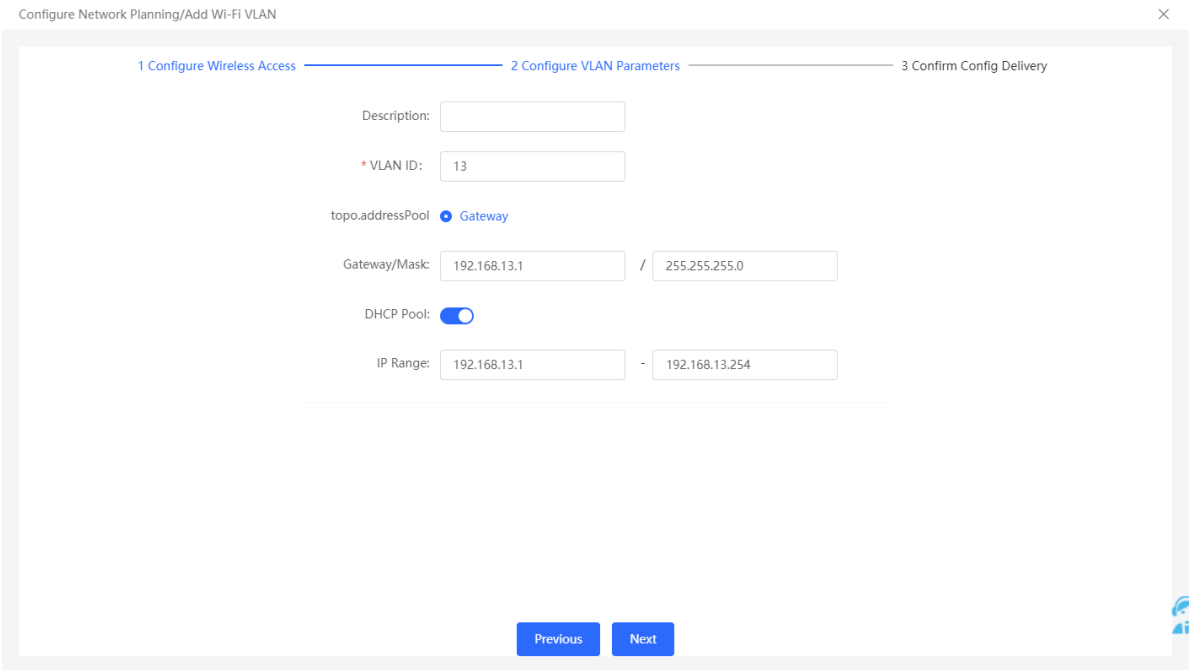
(1) Click **Add Wi-Fi VLAN** to add wireless network configuration, or select an existing Wi-Fi VLAN and click **Setup** to modify its configuration.



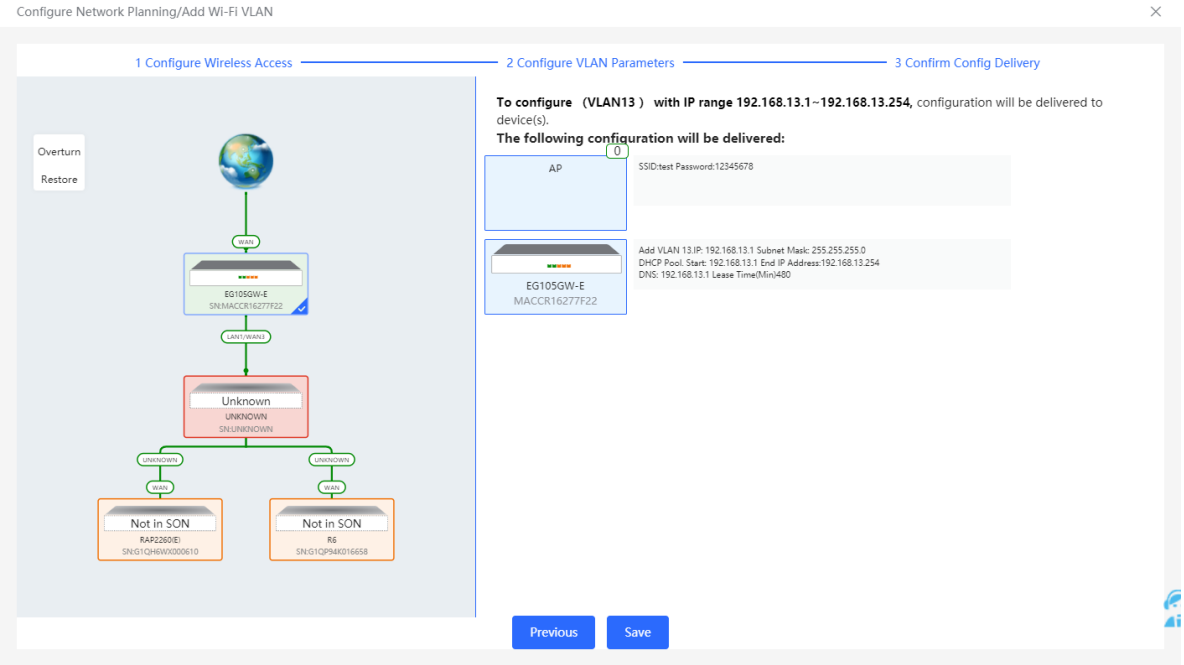
(2) Set the Wi-Fi name, Wi-Fi password, and applicable bands. Click **Next**.



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



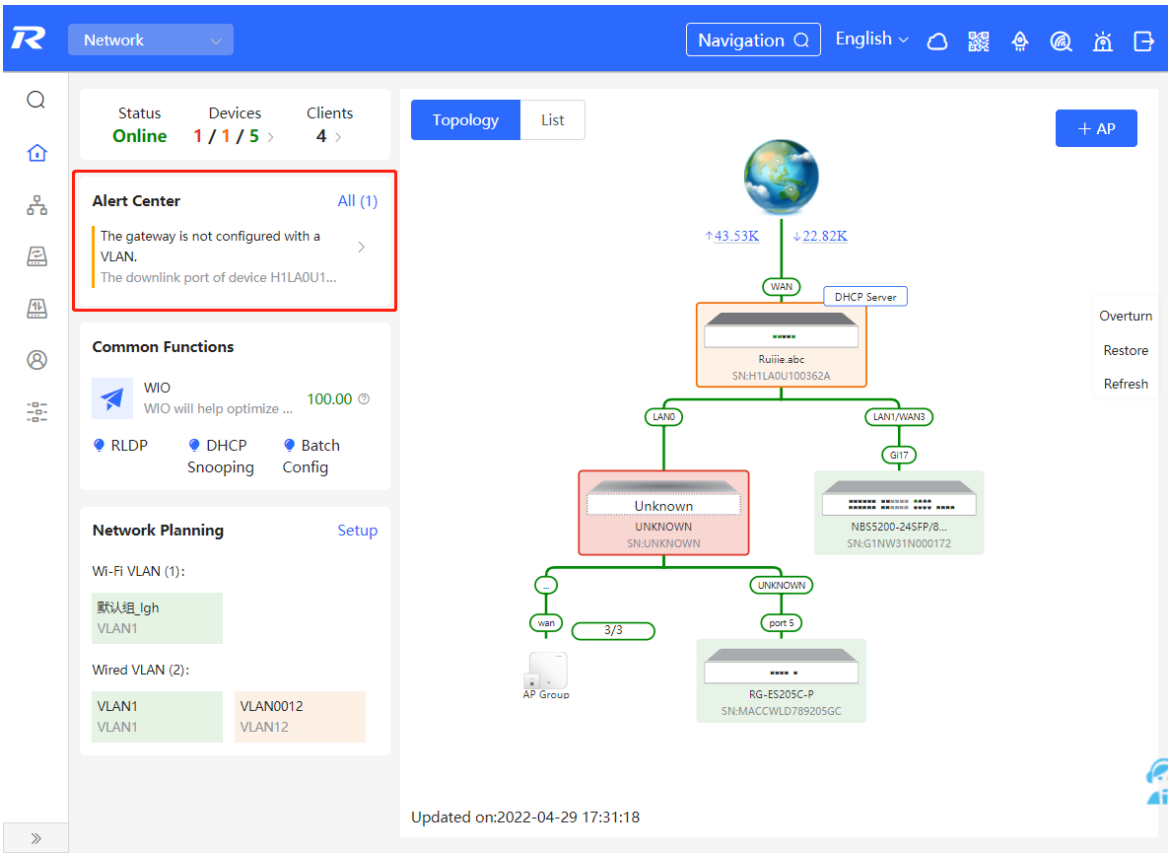
(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.

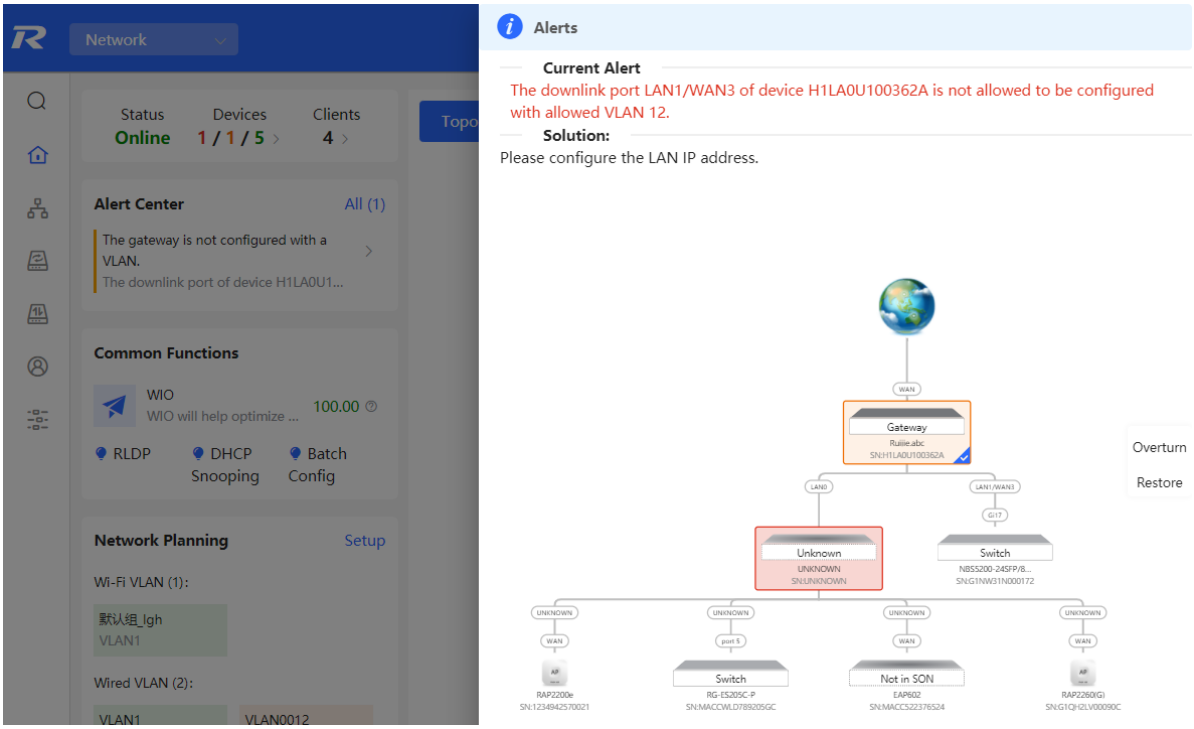


2.6 Processing Alerts

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

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

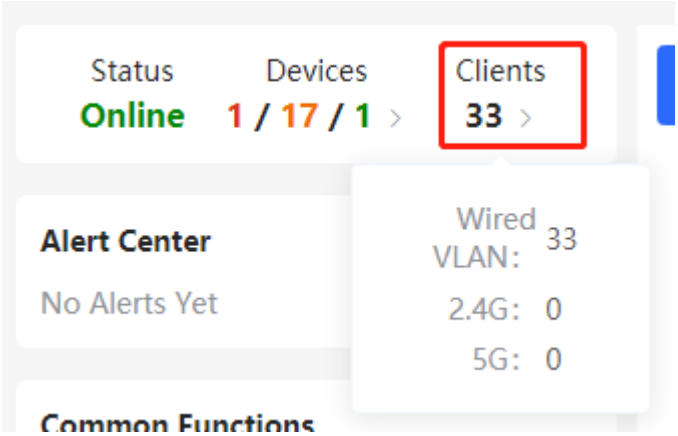

Network
Navigation
English
Status
Online
Devices
1 / 1 / 5
Clients
4
Topology
List
+ AP
Alert Center
All (1)
The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...
Common Functions
WIO
WIO will help optimize ...
100.00
RLDP
DHCP Snooping
Batch Config
Network Planning
Setup
Wi-Fi VLAN (1):
默认组_lgh
VLAN1
Wired VLAN (2):
VLAN1
VLAN1
VLAN0012
VLAN12
↑43.53K
↓22.82K
WAN
DHCP Server
Ruijie.abc
SN:H1LA0U100362A
LAN0
LAN1/WAN3
GI17
Unknown
UNKNOWN
SN:UNKNOWN
NBS5200-24SFP/8...
SN:G1NW31N000172
UNKNOWN
wan
3/3
port 5
AP Group
RG-ES205C-P
SN:MACCWLD789205GC
Overturn
Restore
Refresh
Updated on:2022-04-29 17:31:18


Network
Status
Online
Devices
1 / 1 / 5
Clients
4
Alert Center
All (1)
The gateway is not configured with a VLAN.
The downlink port of device H1LA0U1...
Common Functions
WIO
WIO will help optimize ...
100.00
RLDP
DHCP Snooping
Batch Config
Network Planning
Setup
Wi-Fi VLAN (1):
默认组_lgh
VLAN1
Wired VLAN (2):
Alerts
Current Alert
The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12.
Solution:
Please configure the LAN IP address.
Gateway
Ruijie.abc
SN:H1LA0U100362A
Unknown
UNKNOWN
SN:UNKNOWN
Switch
NBS5200-24SFP/8...
SN:G1NW31N000172
Switch
RG-ES205C-P
SN:MACCWLD789205GC
Not in SON
EAP602
SN:MACC522376524
Overturn
Restore

2.7 Viewing Online Clients

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

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



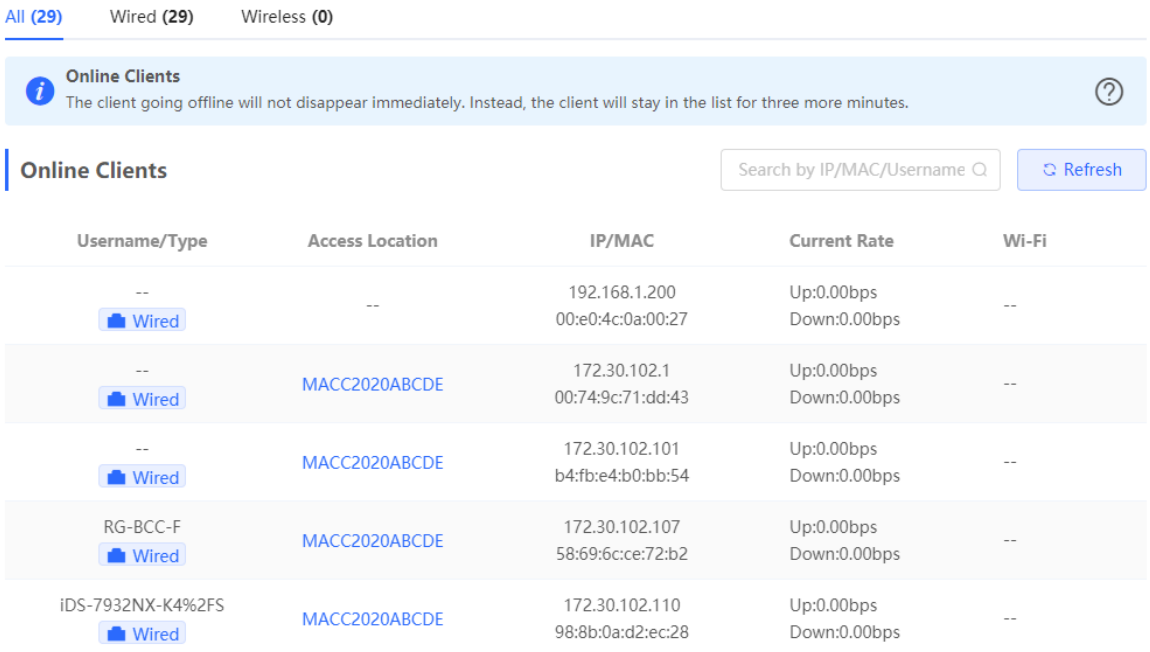


Table 2-1 Description of Online Client Information

Field	Description
Username/Type	Indicate the name and access type of the client. The access type can be wireless or wired.

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

2.8 Smart Device Network

Caution

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

2.8.1 Overview

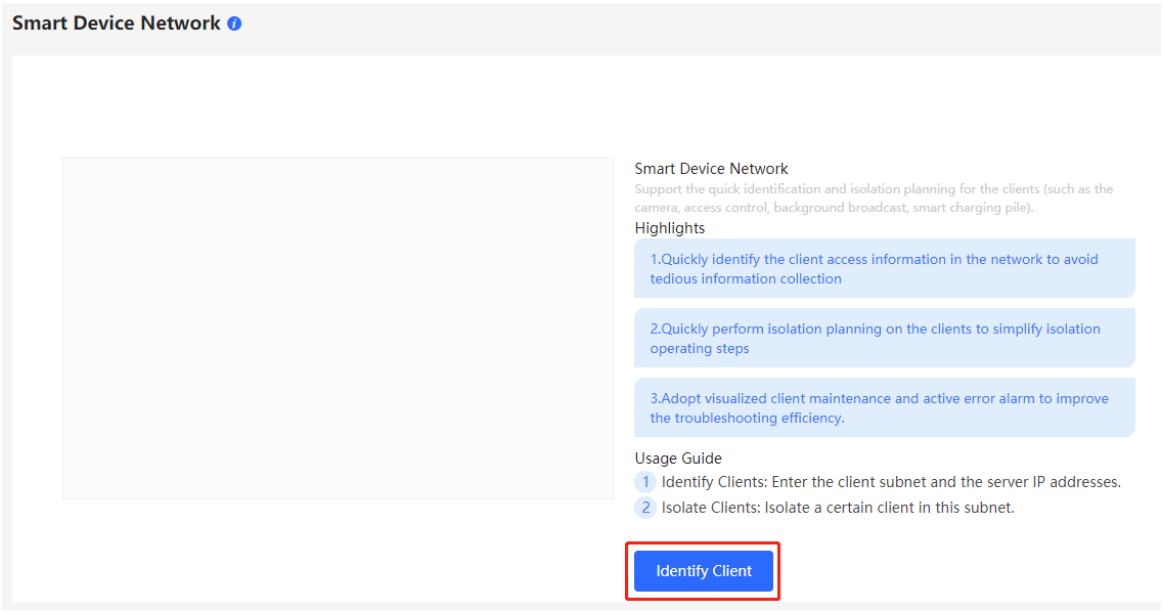
The smart device network is used to quickly plan and set up an isolation network for smart clients, so as to isolate the client network from the normal service network and other types of clients, and improve the stability of the network. The smart device network supports rapid identification of various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

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

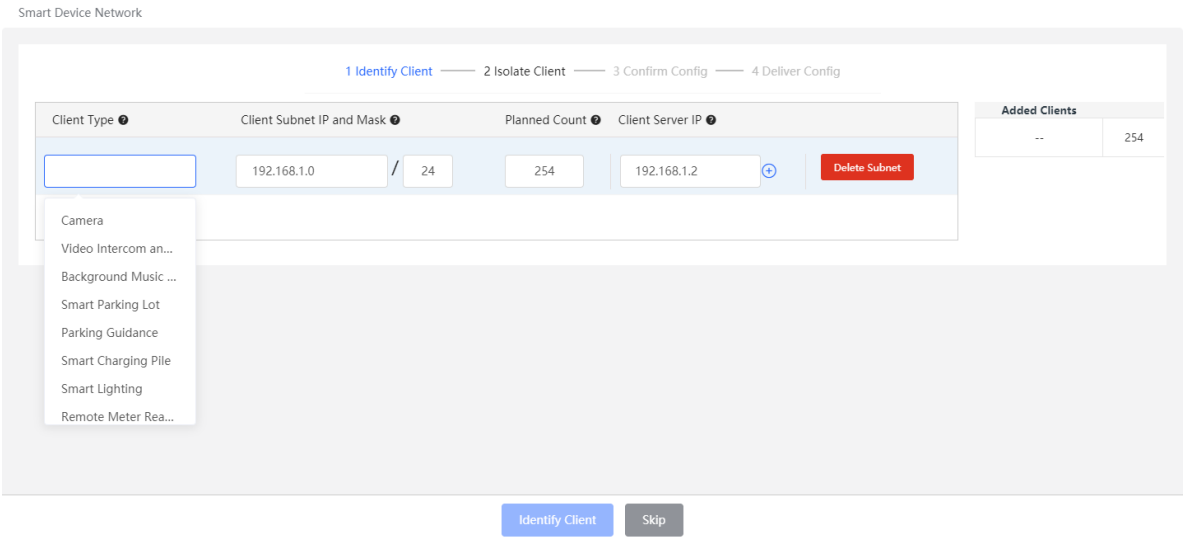
2.8.2 Procedure

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

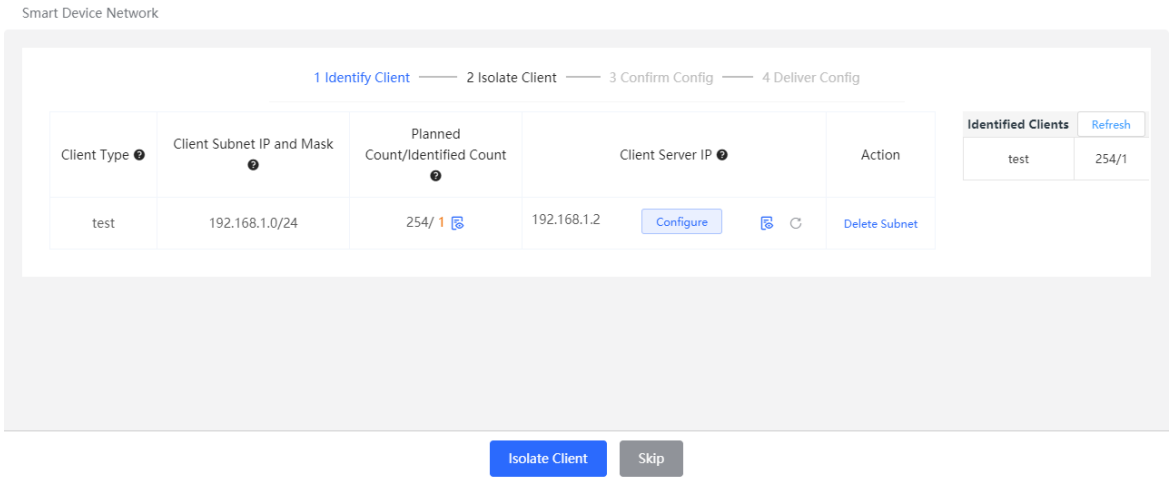
(1) Click **Identify Client**.

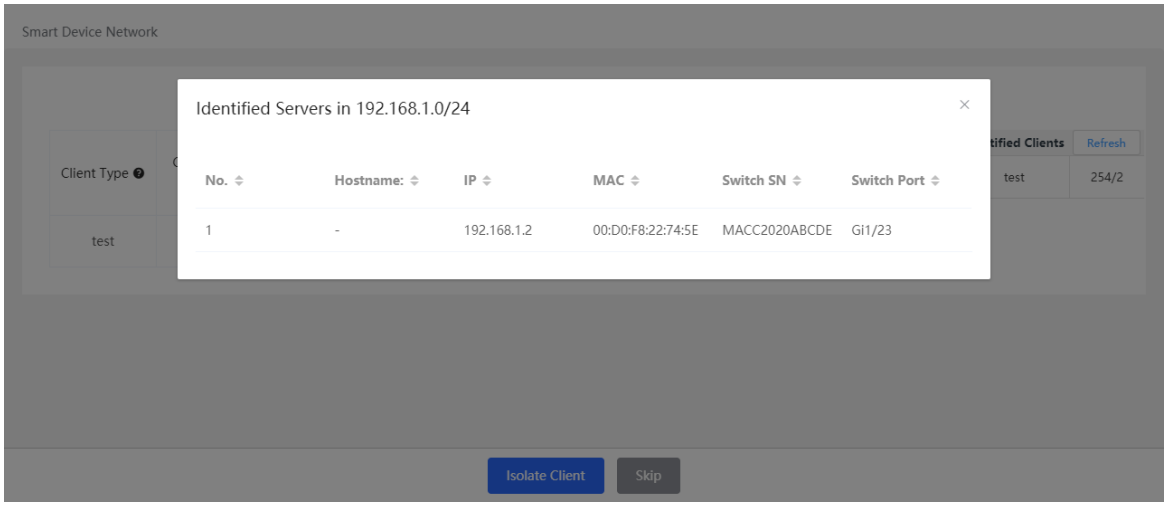


(2) Click **+Client Subnet**, enter the client type (which can be selected or customized in the drop-down box), the network segment of the client, the planned number and the corresponding server IP address to identify the client. Multi-type client network segments can be set. Click **Identify Client**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

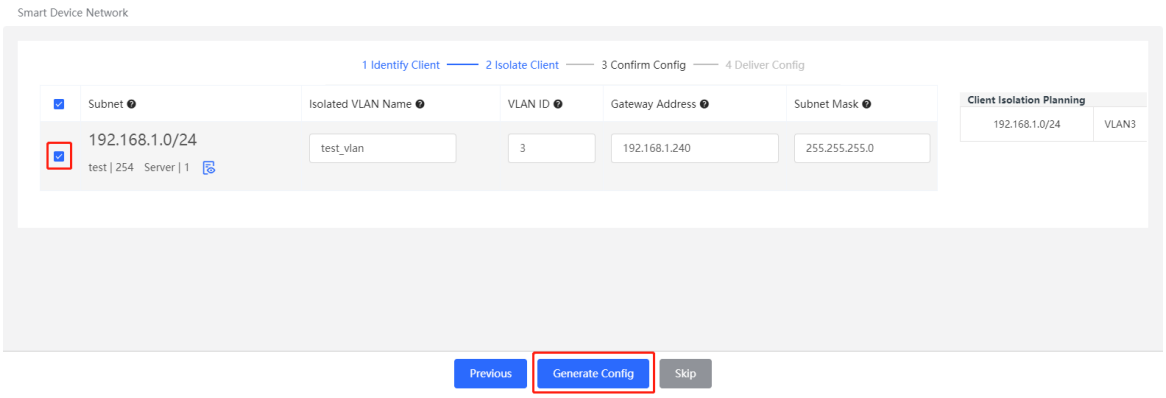


(3) Display the identified client and client server information, including IP address, MAC address, SN number of the connected switch and connection port. Click to view the detailed information. If the connection information to the client server is not identified, you need to click **Configure** and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

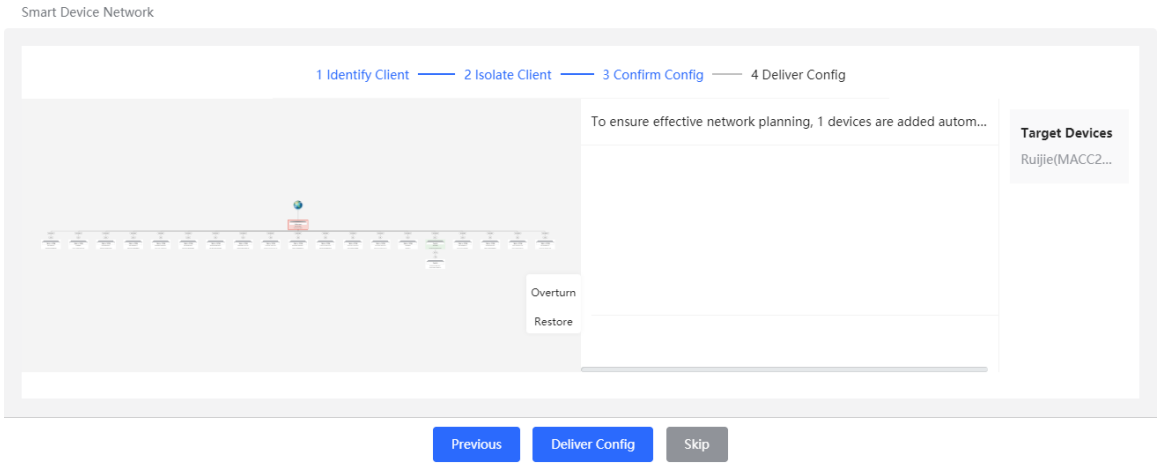




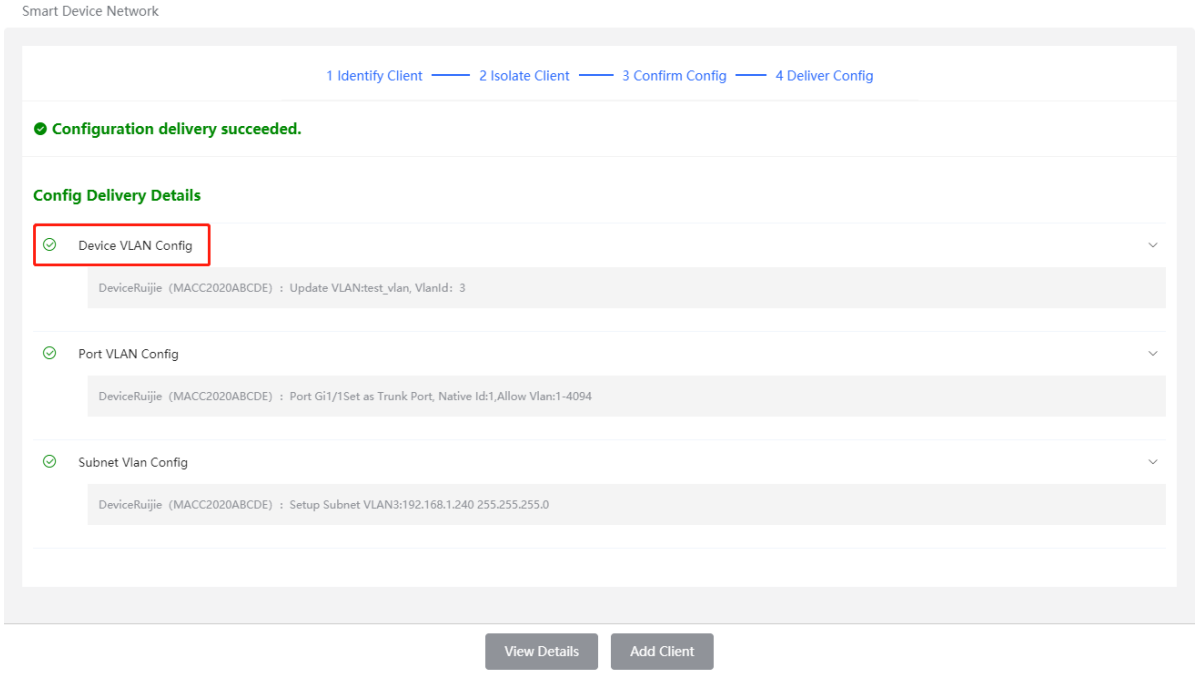
(4) Input the name of the VLAN, VLAN ID, gateway address, and subnet mask of the isolated client. Check the target network segment and click **Generate Config**.



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



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



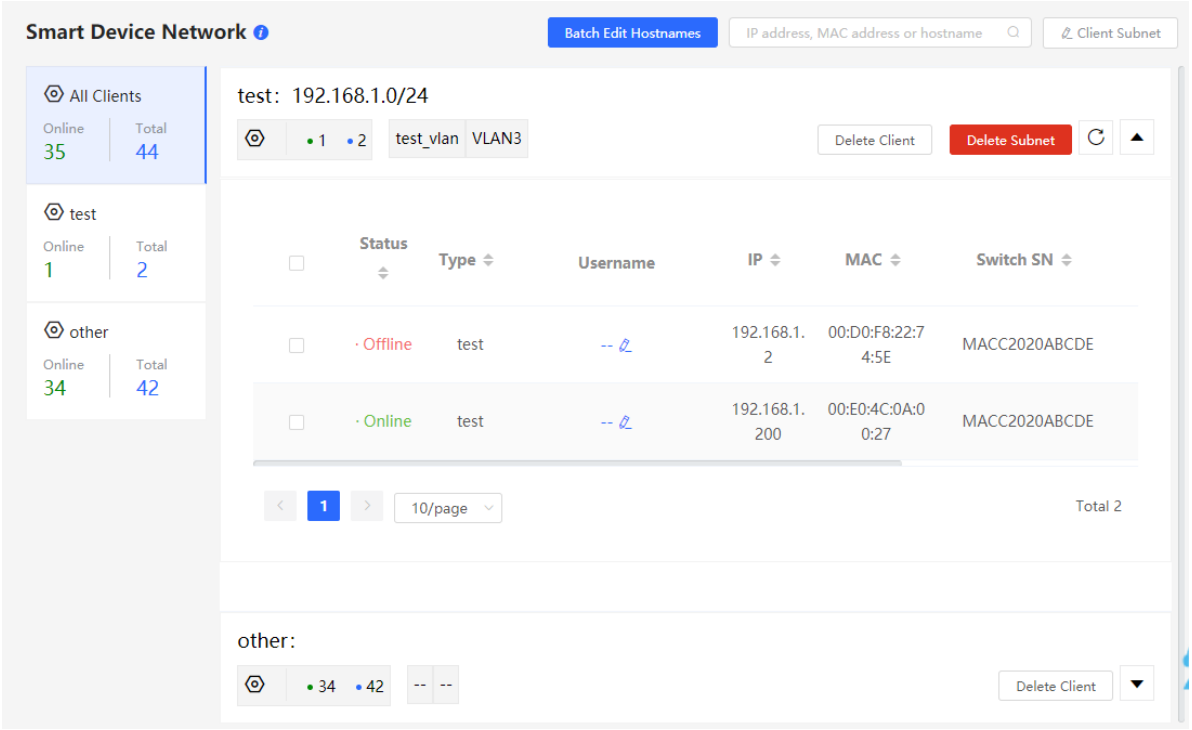
(7) After completing the smart device network settings, you can view the client monitoring information on the page, including client online status, connection information, device information, and online and offline time.

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

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

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

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



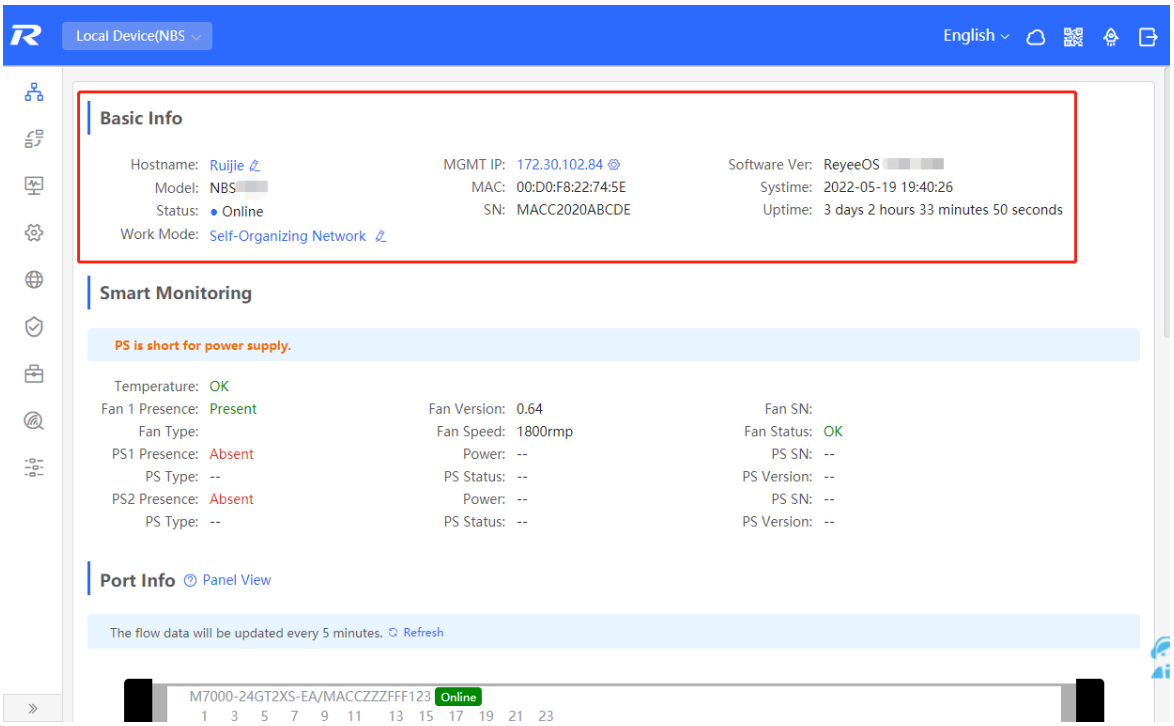
3 Basic Management

3.1 Overviewing Switch Information

3.1.1 Basic information about the Device

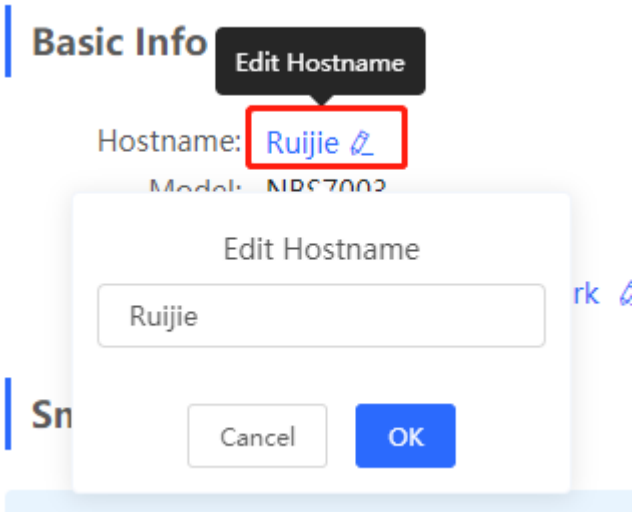
Choose **Local Device** > **Home** > **Basic Info**.

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



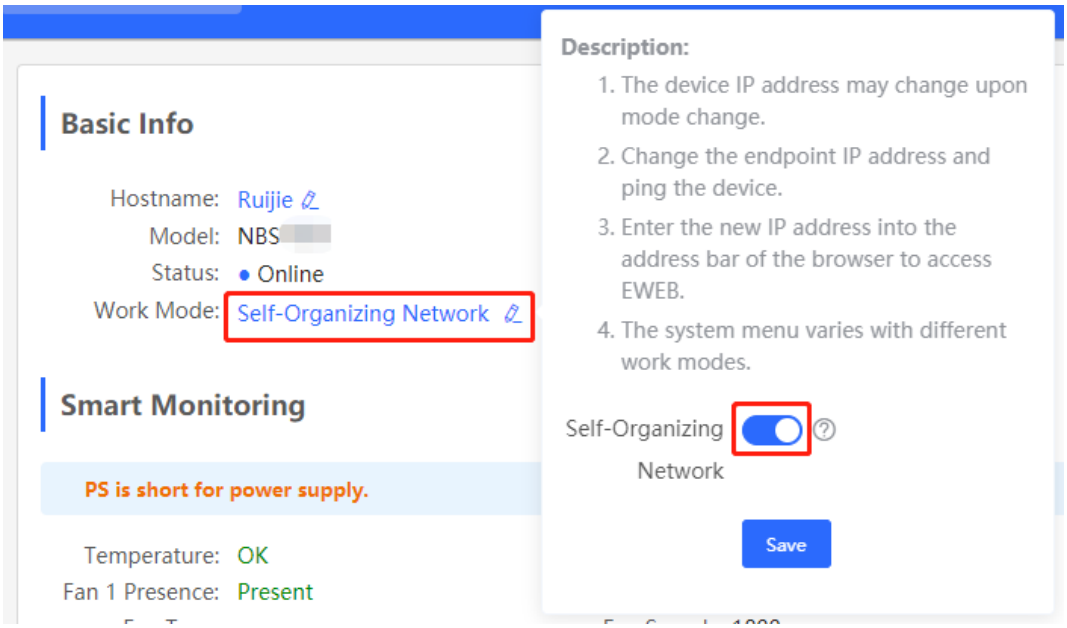
1. Setting the device name

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



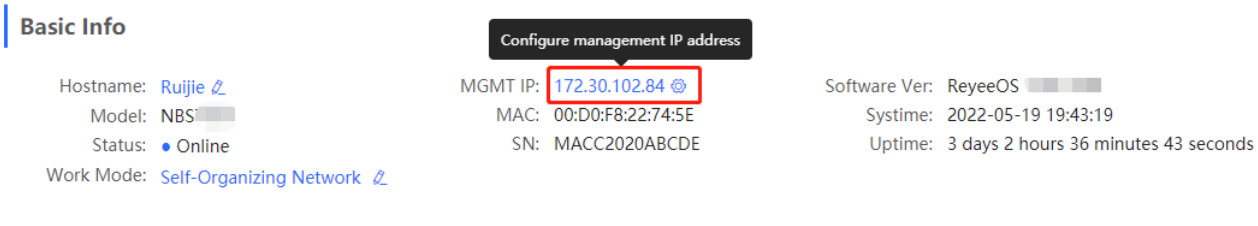
2. Switching the Work Mode

Click the current work mode to change the work mode.



3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see 4.6 .



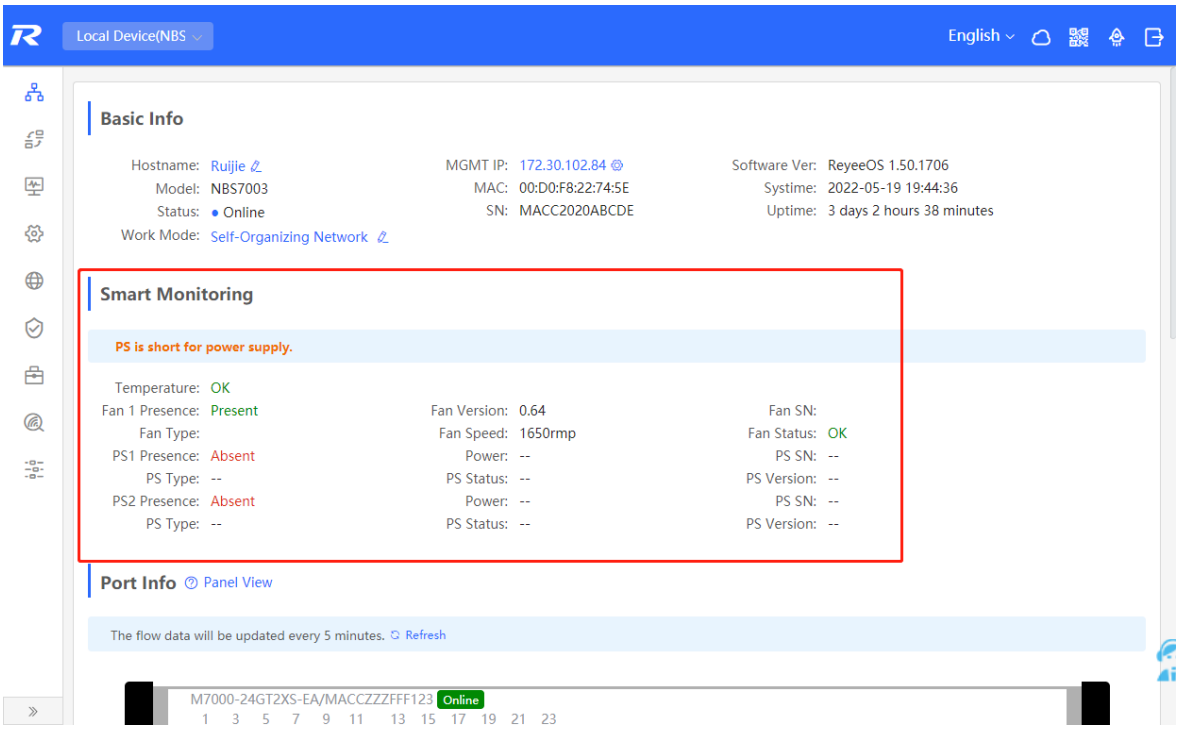
3.1.2 Hardware Monitor Information

Caution

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

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

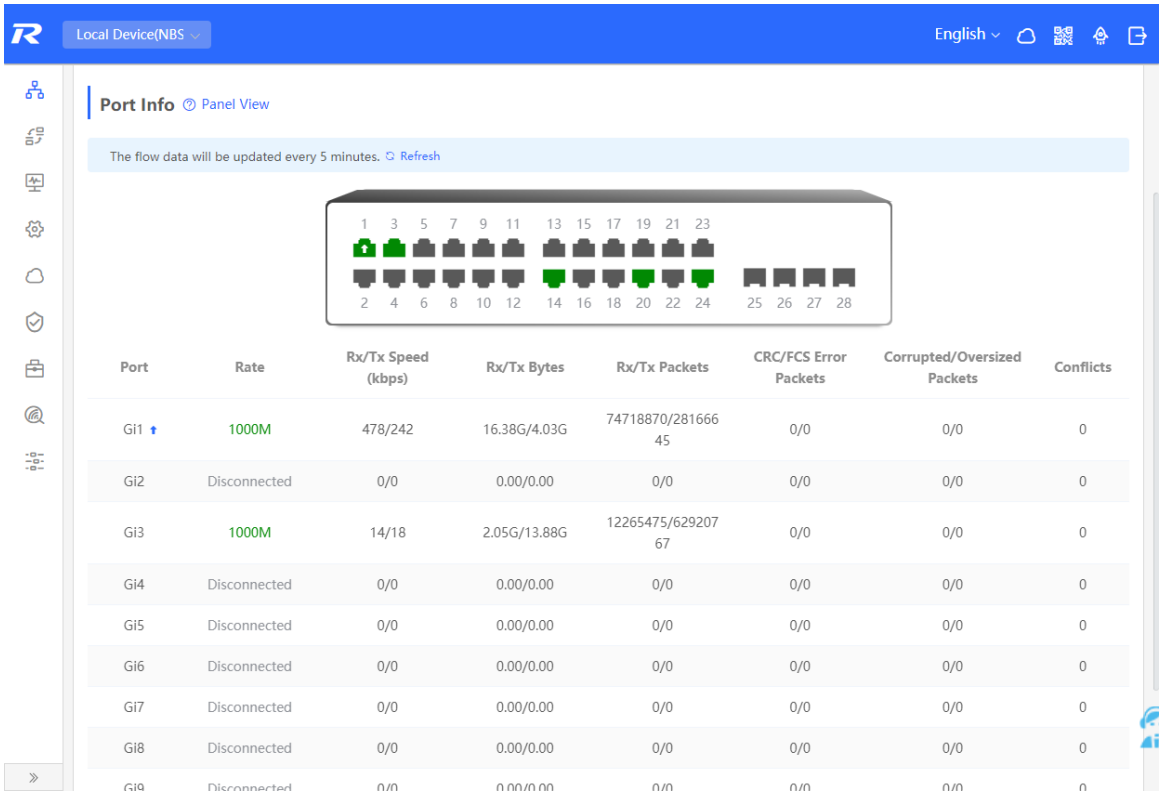
Display the current hardware operating status of the device, such as the device temperature and power supply status, etc.



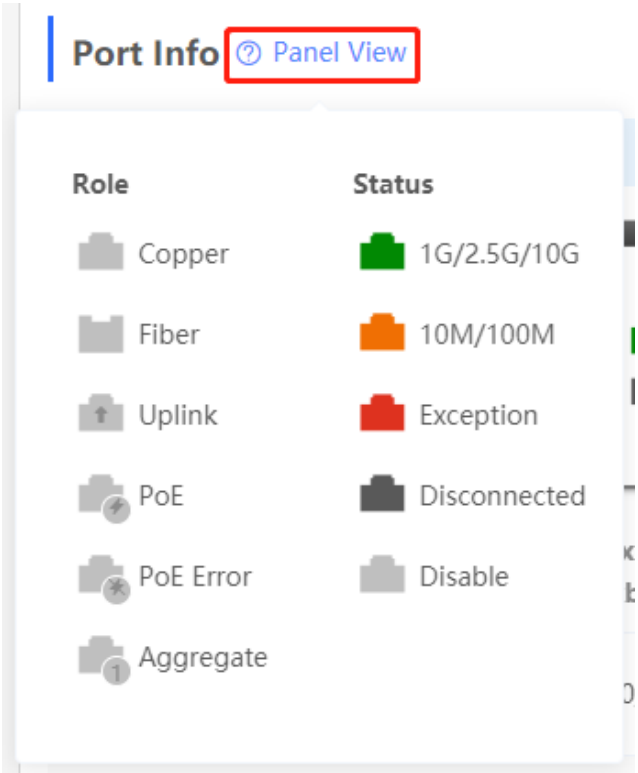
3.1.3 Port Info

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

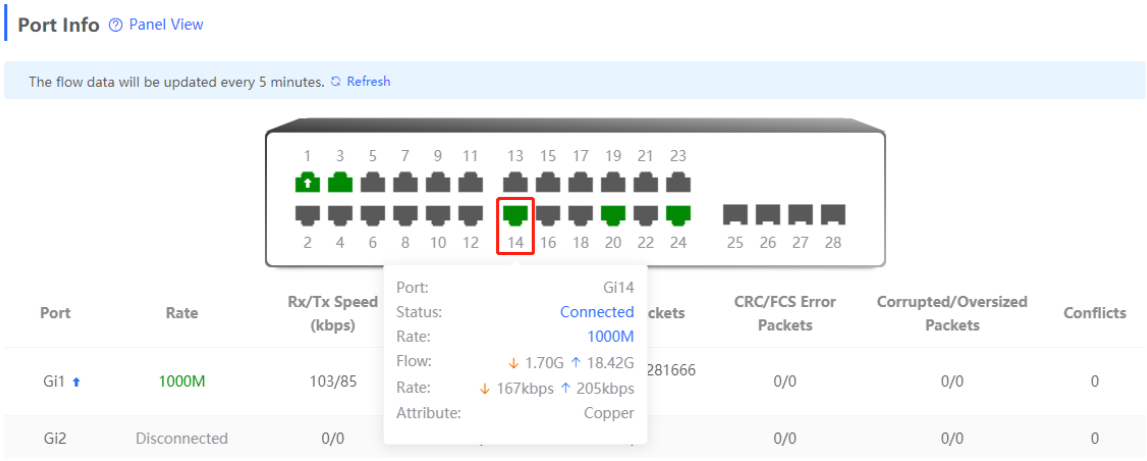
- The port info page displays the details of all ports currently on the switch. Click **Panel View** to view the port roles and statuses corresponding to port icons of different colors or shapes.



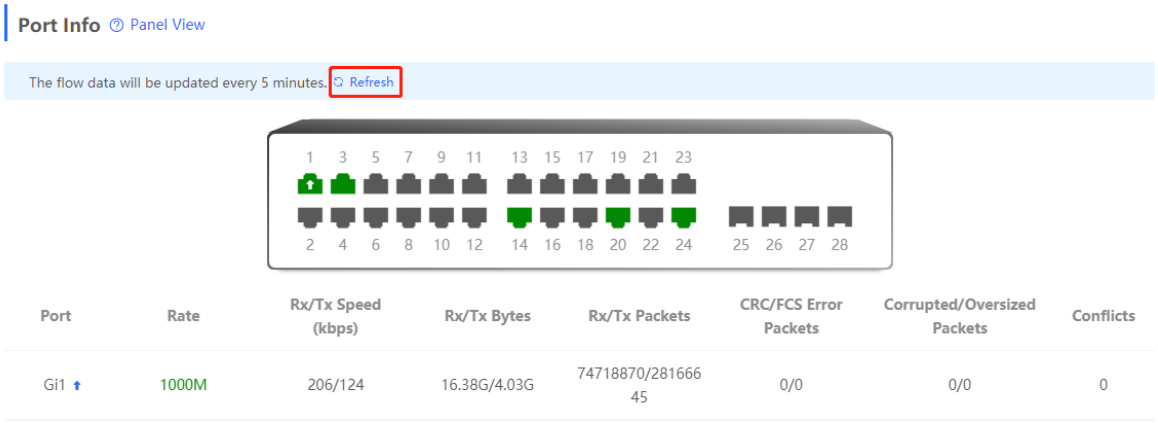
Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1	1000M	478/242	16.38G/4.03G	74718870/28166645	0/0	0/0	0
Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi3	1000M	14/18	2.05G/13.88G	12265475/62920767	0/0	0/0	0
Gi4	Disconnected	0/0	0.00/0.00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



- 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.



- 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.



3.2 Port Flow Statistics

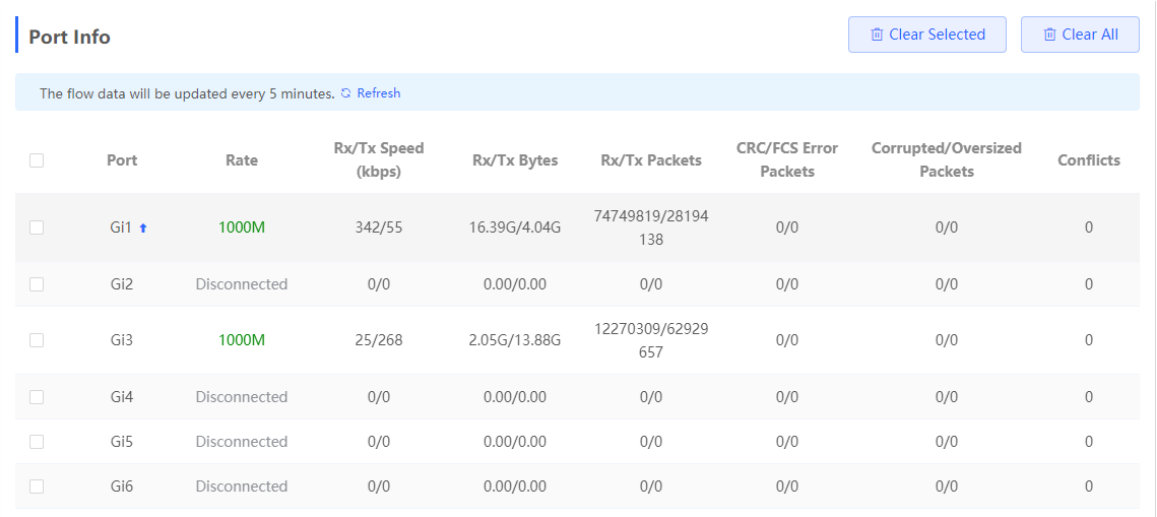
Choose **Local Device** > **Monitor** > **Port Flow**.

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

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

Note

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



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

3.3 MAC Address Management

3.3.1 Overview

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

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

MAC address entries are classified into the following types:

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

Note

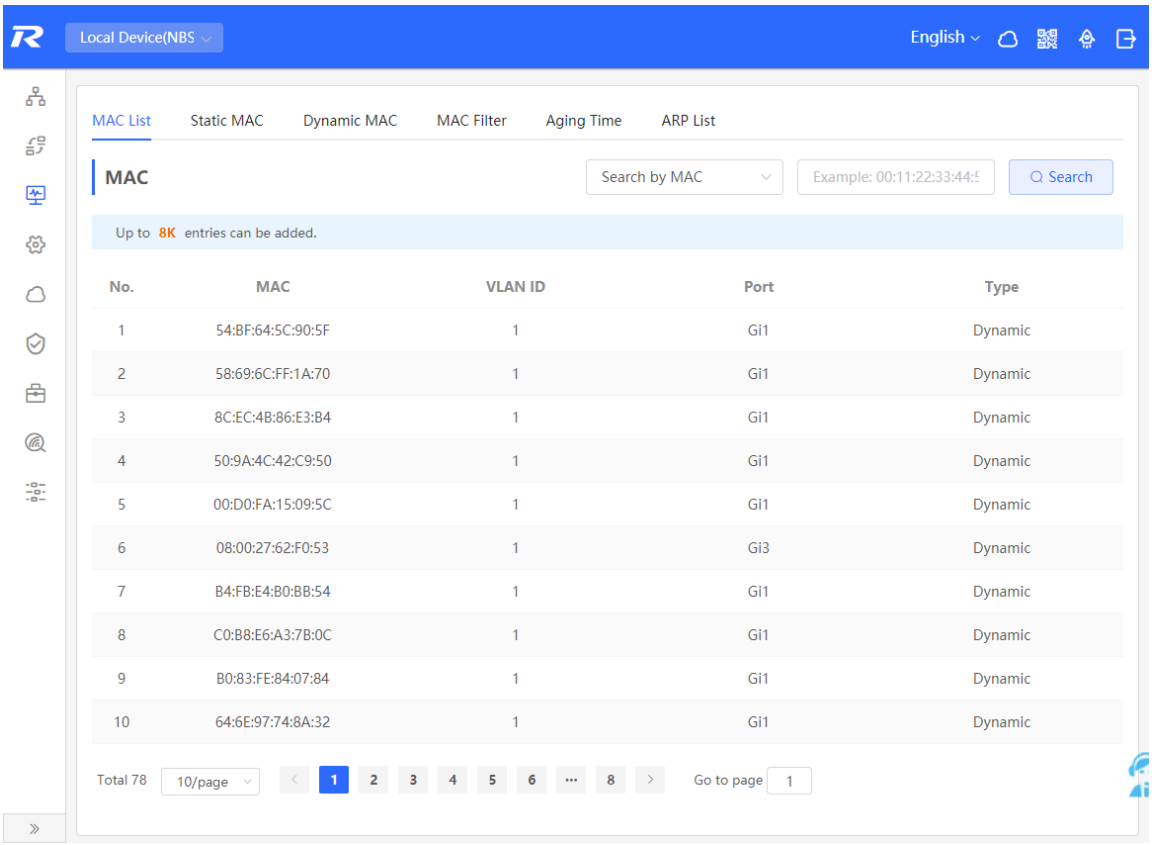
This section describes the management of static, dynamic, and filtering MAC address entries, without involving multicast MAC address entries.

3.3.2 Displaying the MAC Address Table

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

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

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



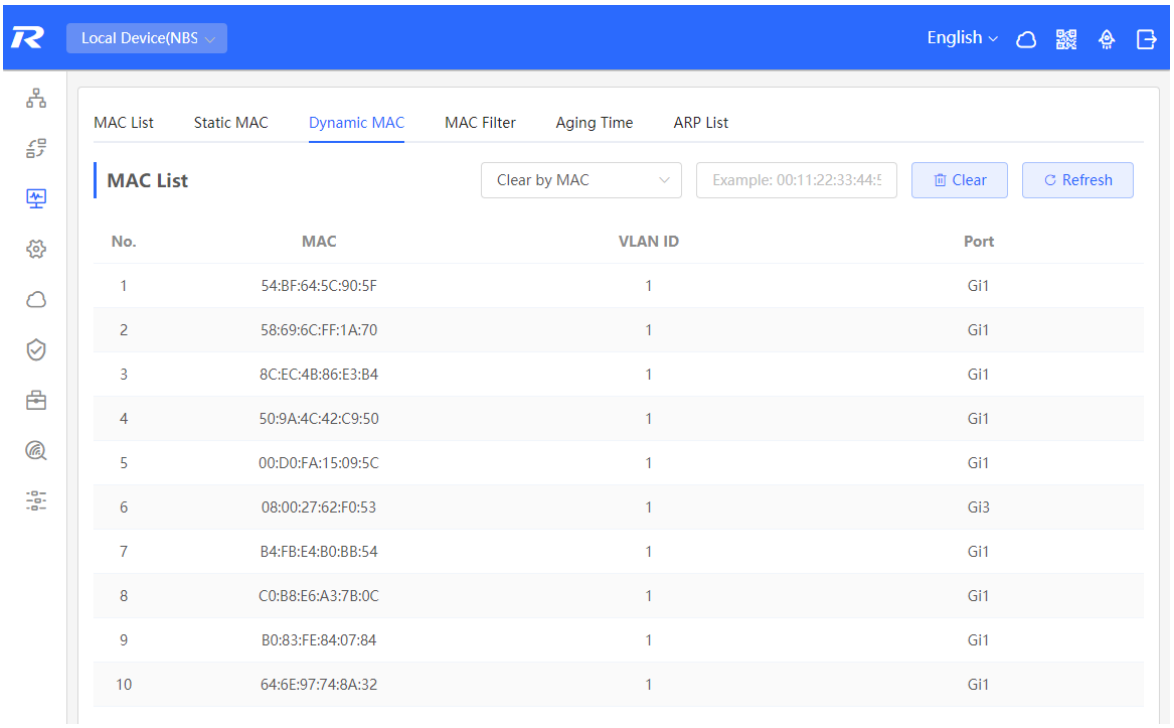
Note

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

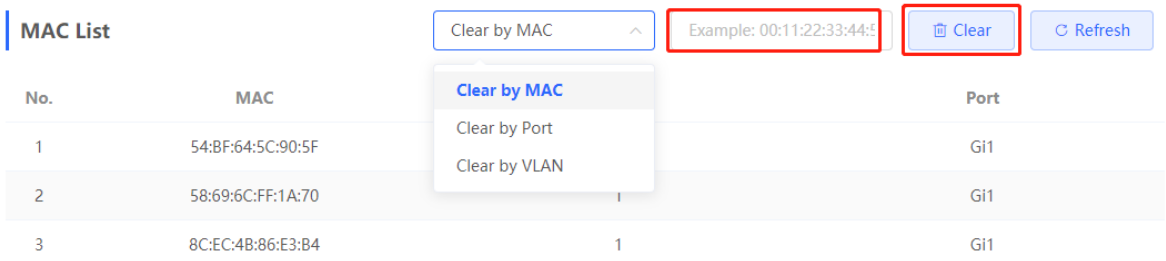
3.3.3 Displaying Dynamic MAC Address

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

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

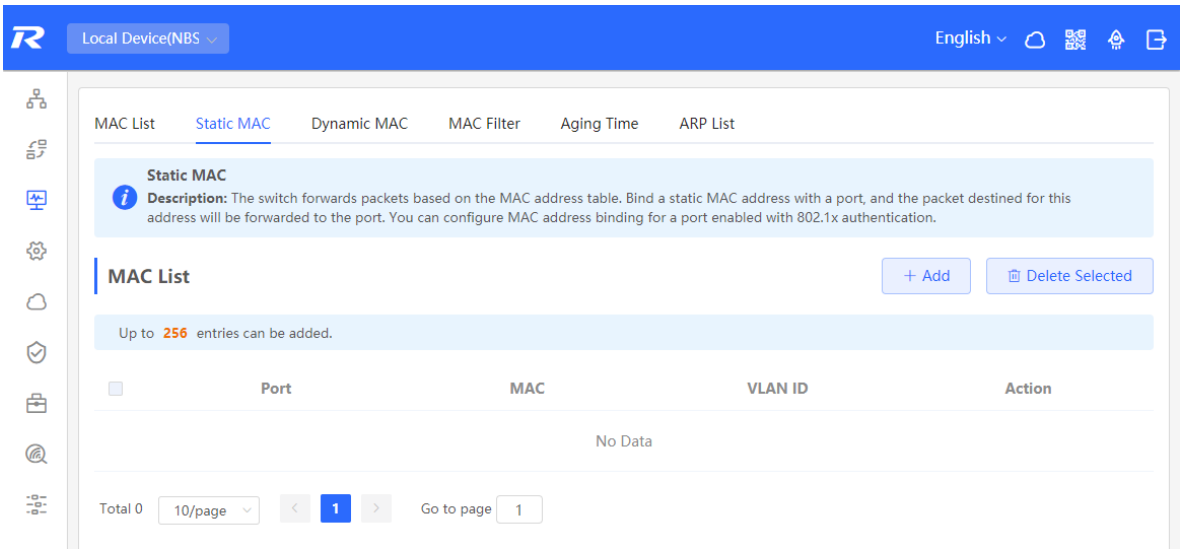


Delete dynamic MAC address: Select the clear type (by MAC address, by VLAN, or by port), enter a string for matching the dynamic MAC address entry, and click **Clear**. The device will clear MAC address entries that meet the conditions.



3.3.4 Configuring Static MAC Binding

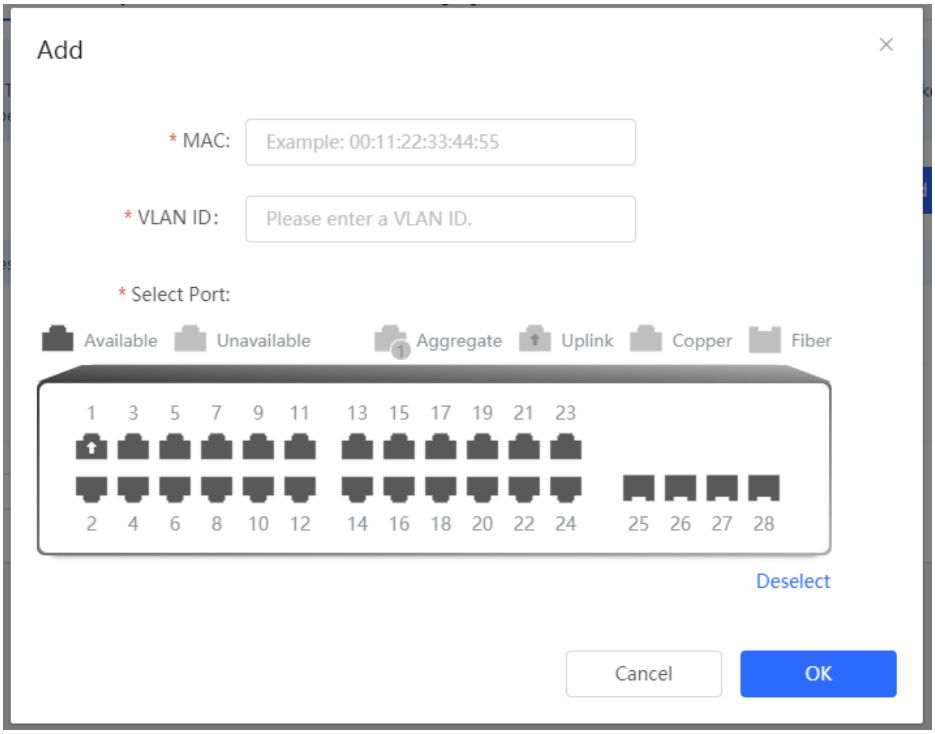
The switch forwards data based on the MAC address table. You can set a static MAC address entry to manually bind the MAC address of a downlink network device with the port of the device. After a static address entry is configured, when the device receives a packet destined to this address from the VLAN,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



1. Adding Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients** > **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 update the entry data.

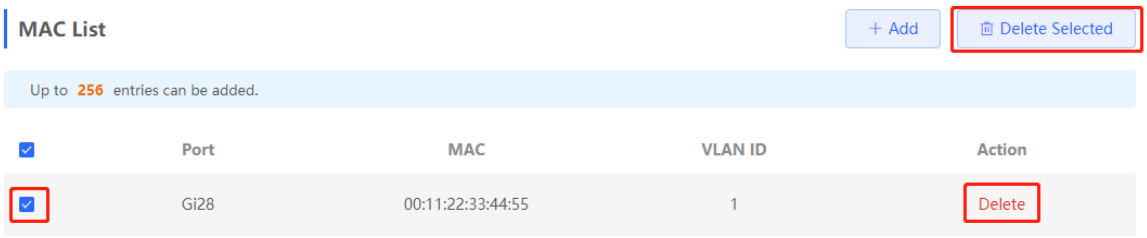


2. Deleting Static MAC Address Entries

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

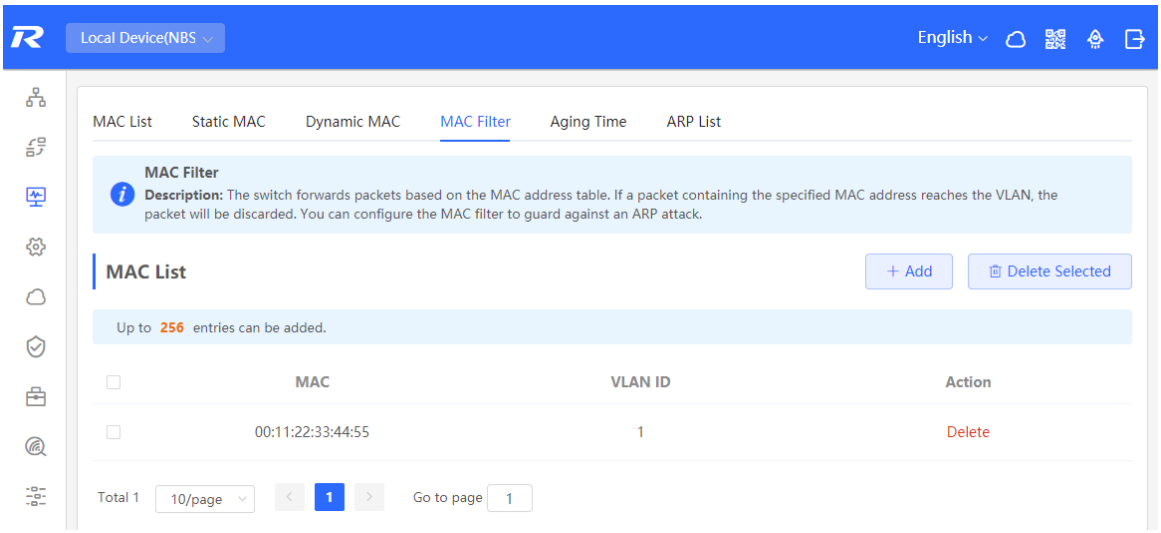
Batch delete: In **MAC List**, select the MAC address entries to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.

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



3.3.5 Configuring MAC Address Filtering

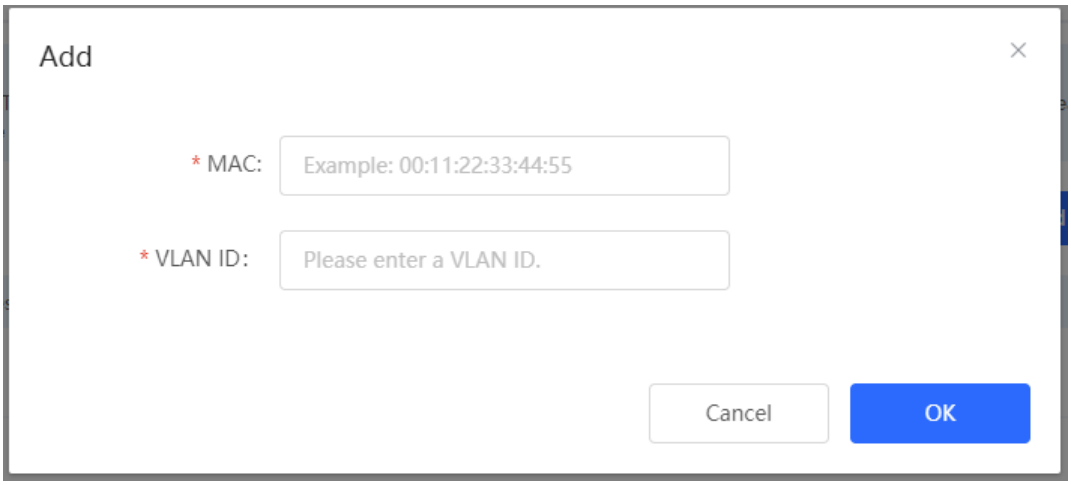
To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly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



1. Adding Filtering MAC Address

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

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

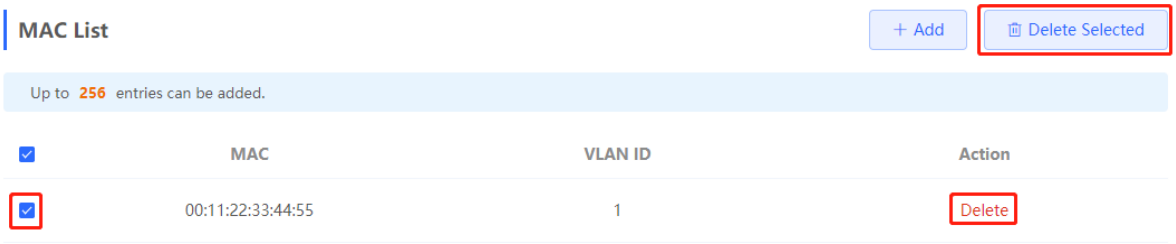


2. MAC Filter

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

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

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



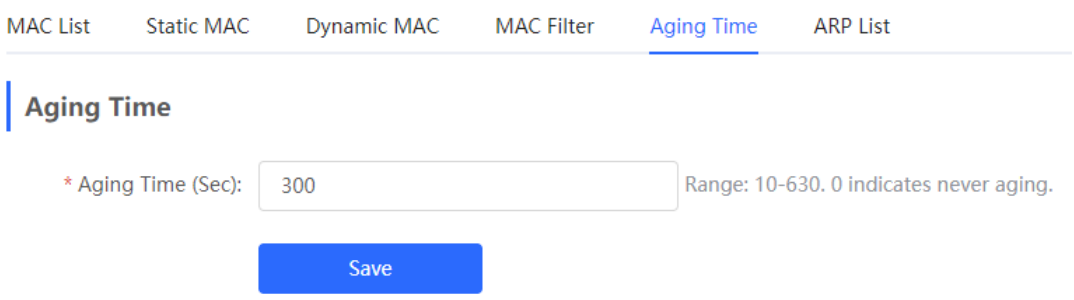
3.3.6 Configuring MAC Address Aging Time

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

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

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

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



3.4 Displaying ARP Information

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

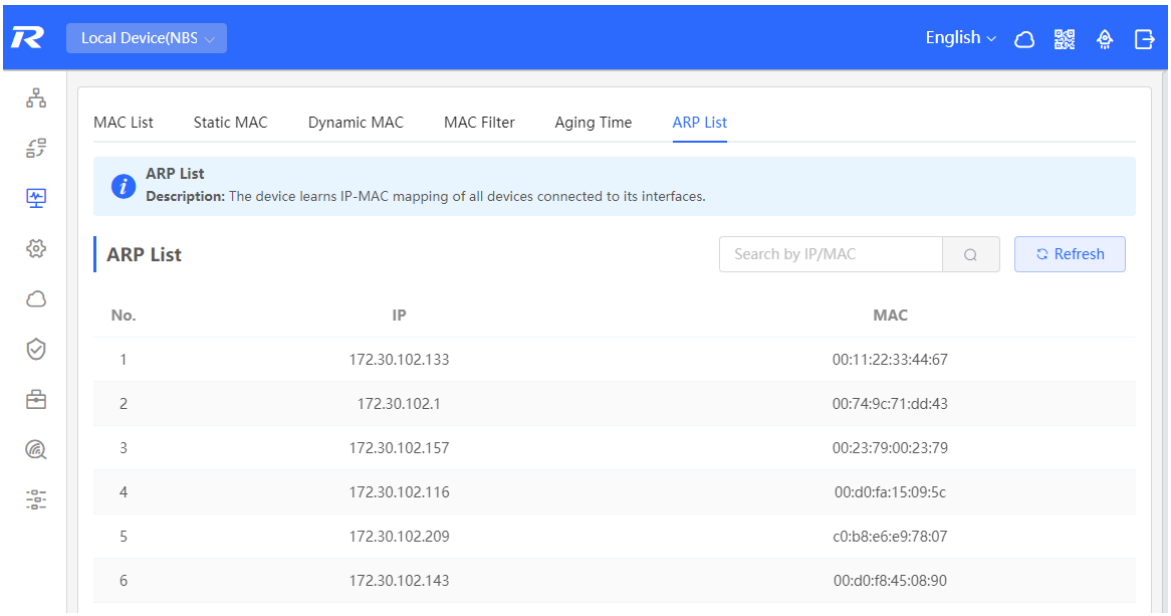
When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then send data frames to the physical network. The process of obtaining MAC addresses based on IP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

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

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

Note

For more ARP entry function introduction, see 6.6 .



3.5 VLAN

3.5.1 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.

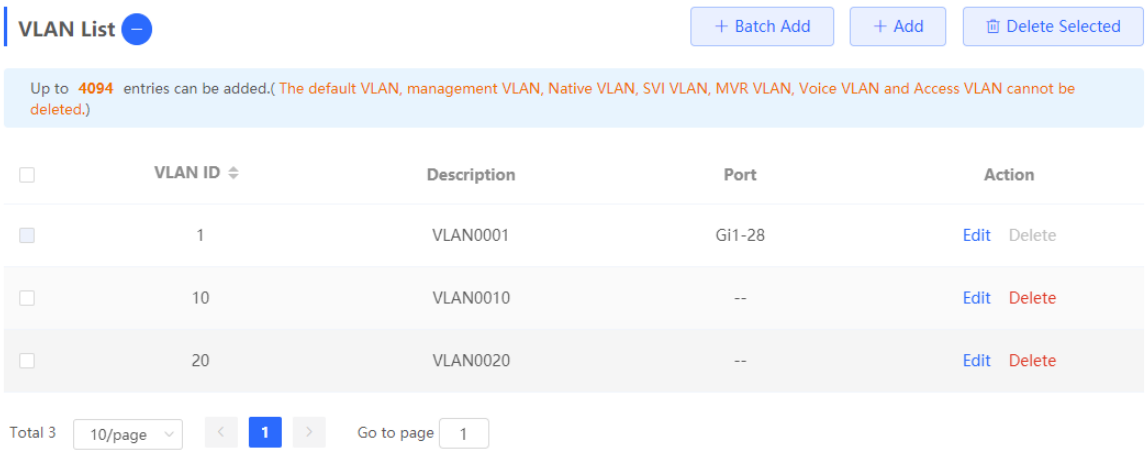
When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs. VLANs can make L3 communication with each other through L3 devices or L3 interfaces.

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

3.5.2 Creating a VLAN

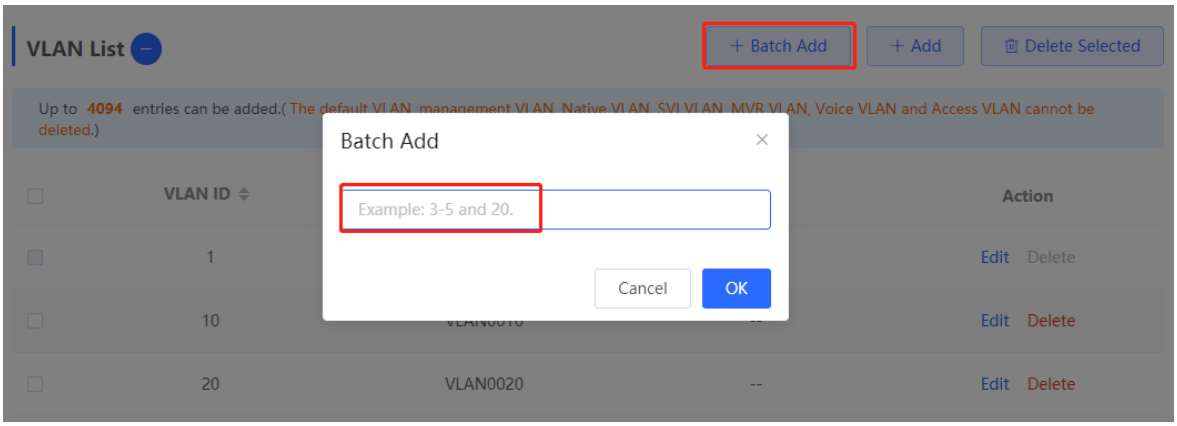
Choose **Local Device** > **VLAN** > **VLAN List**.

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

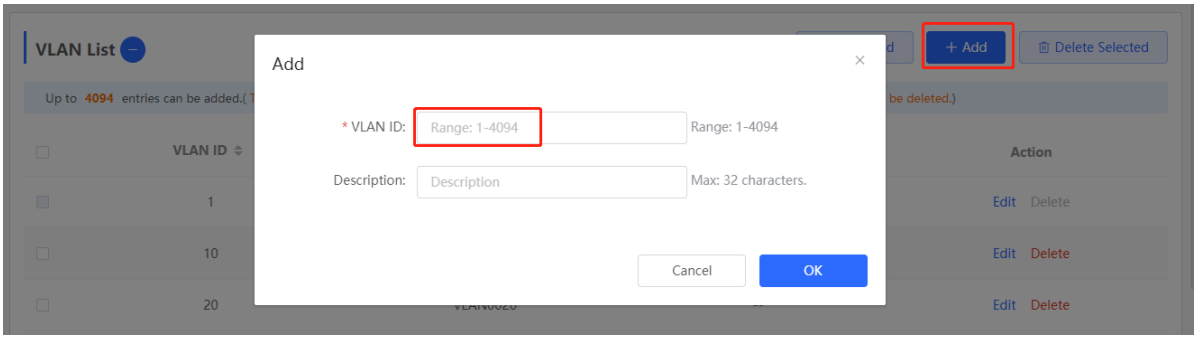


1. Adding a VLAN

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



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



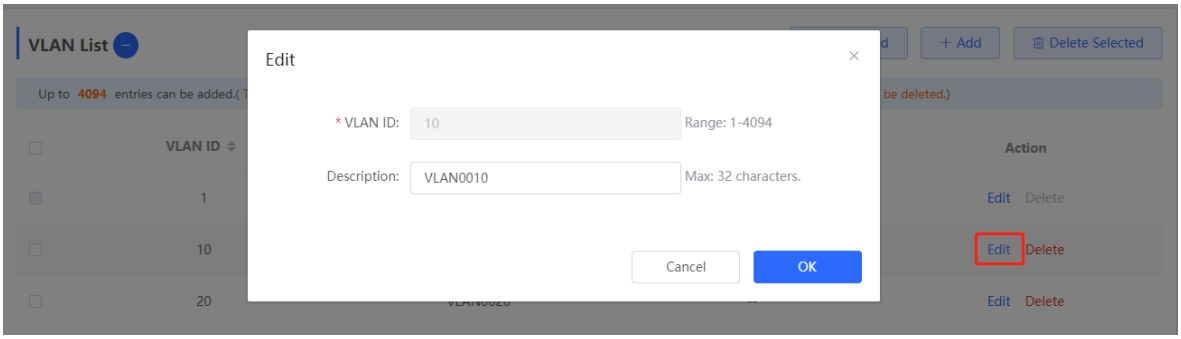
Note

- The range of a VLAN ID is from 1 to 4094.

- You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).
- If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.
- If the device supports L3 functions, VLANs, routed ports, and L3 aggregate ports (L3APs) share limited hardware resources. If resources are insufficient, a message indicating resource insufficiency for VLAN will be displayed.

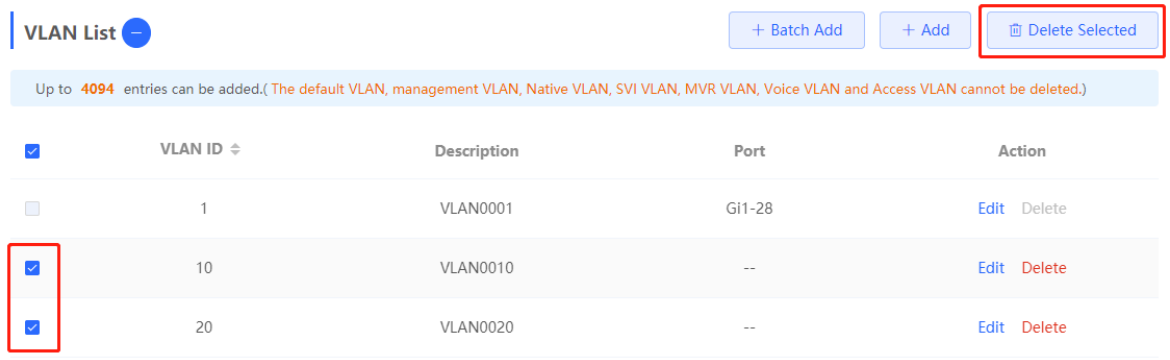
2. VLAN Description Modifying

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

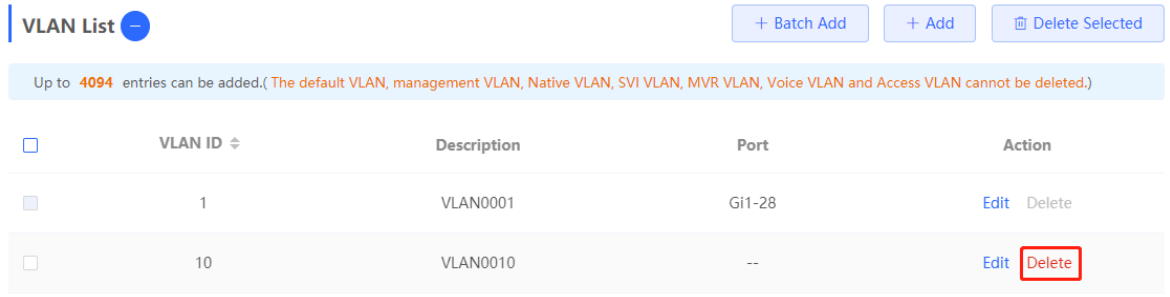


3. Deleting a VLAN

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



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



Note

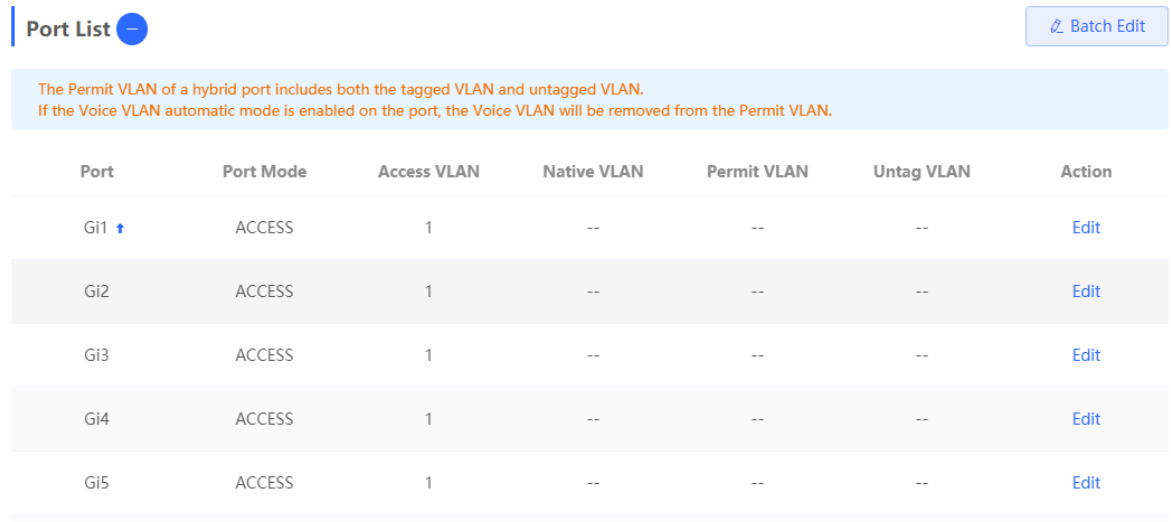
The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. For these VLANs, the **Delete** button is unavailable in gray.

3.5.3 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.



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 3-1 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

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

Note

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

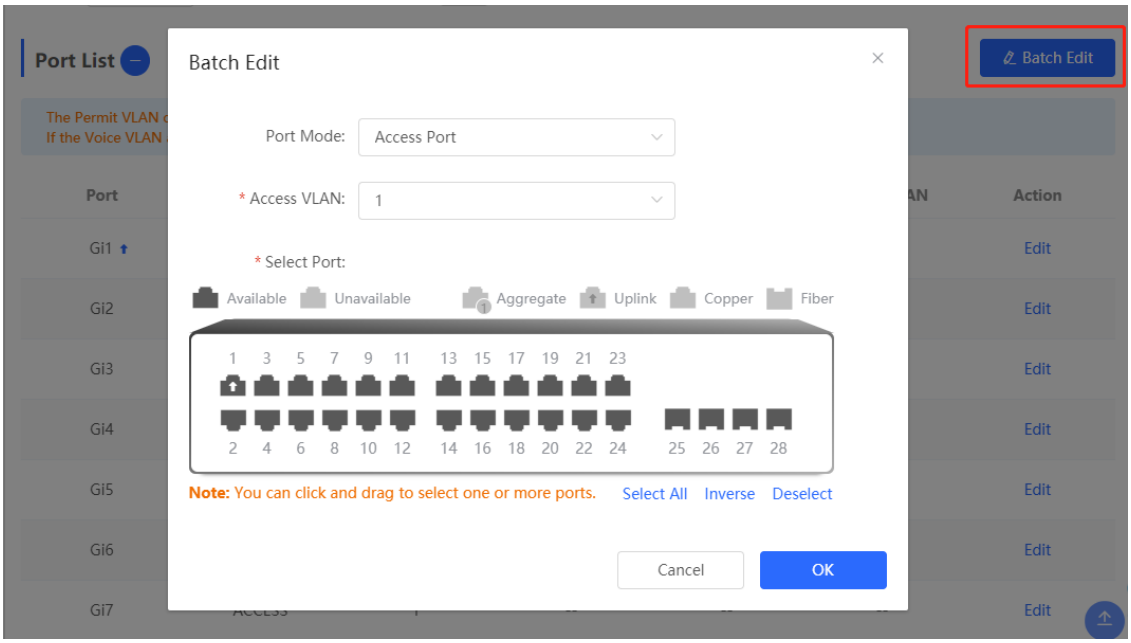
2. Procedure

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

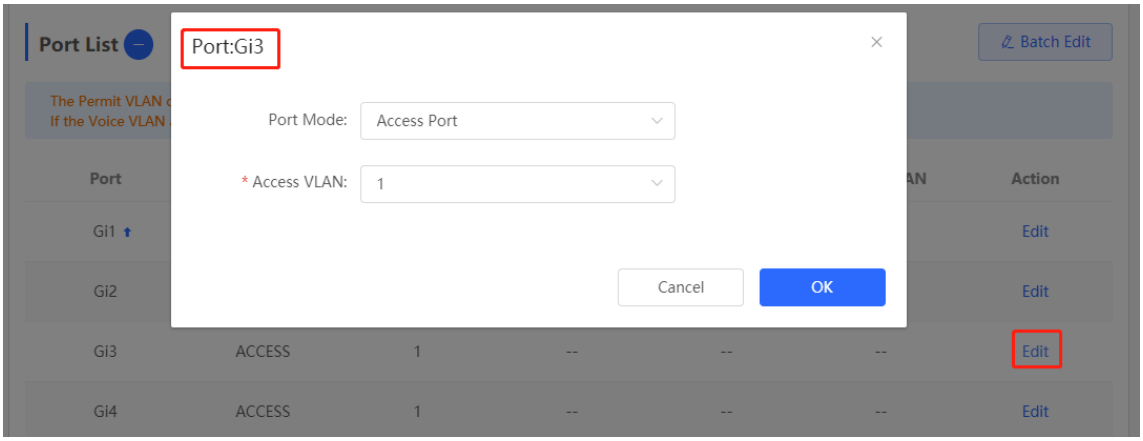
Configure port VLANs in a batch: Click **Batch Edit**, select the port to be configured on the port panel, and select the port mode. If the port mode is Access port, you need to select Access VLAN; if the port mode is Trunk port, you need to select Native VLAN and enter the allowed VLAN ID range; if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

Note

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



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



Note

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

3.5.4 Batch Switch Configuration

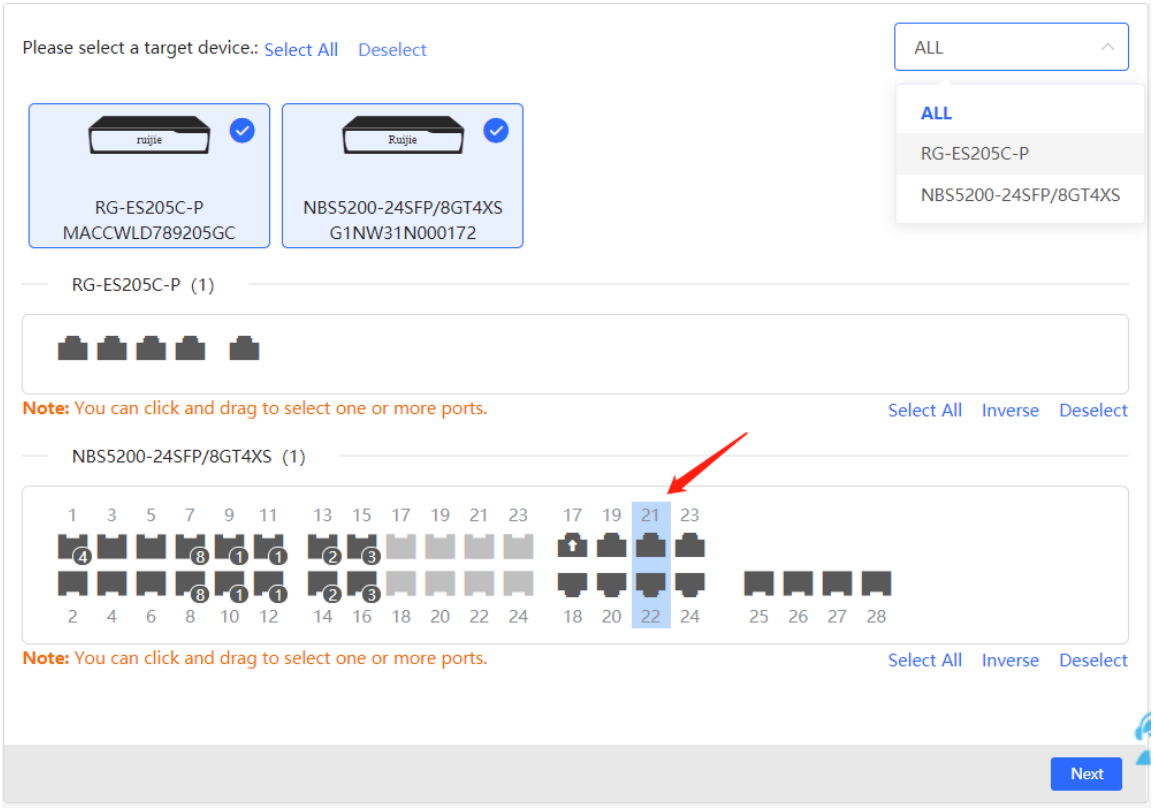
1. Overview

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

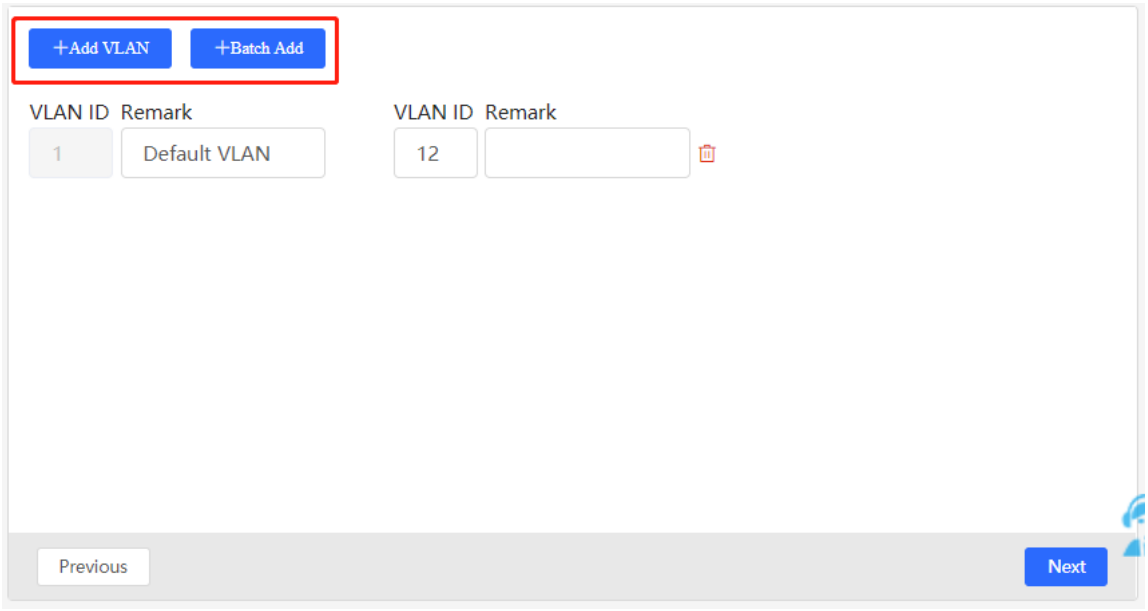
2. Procedure

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

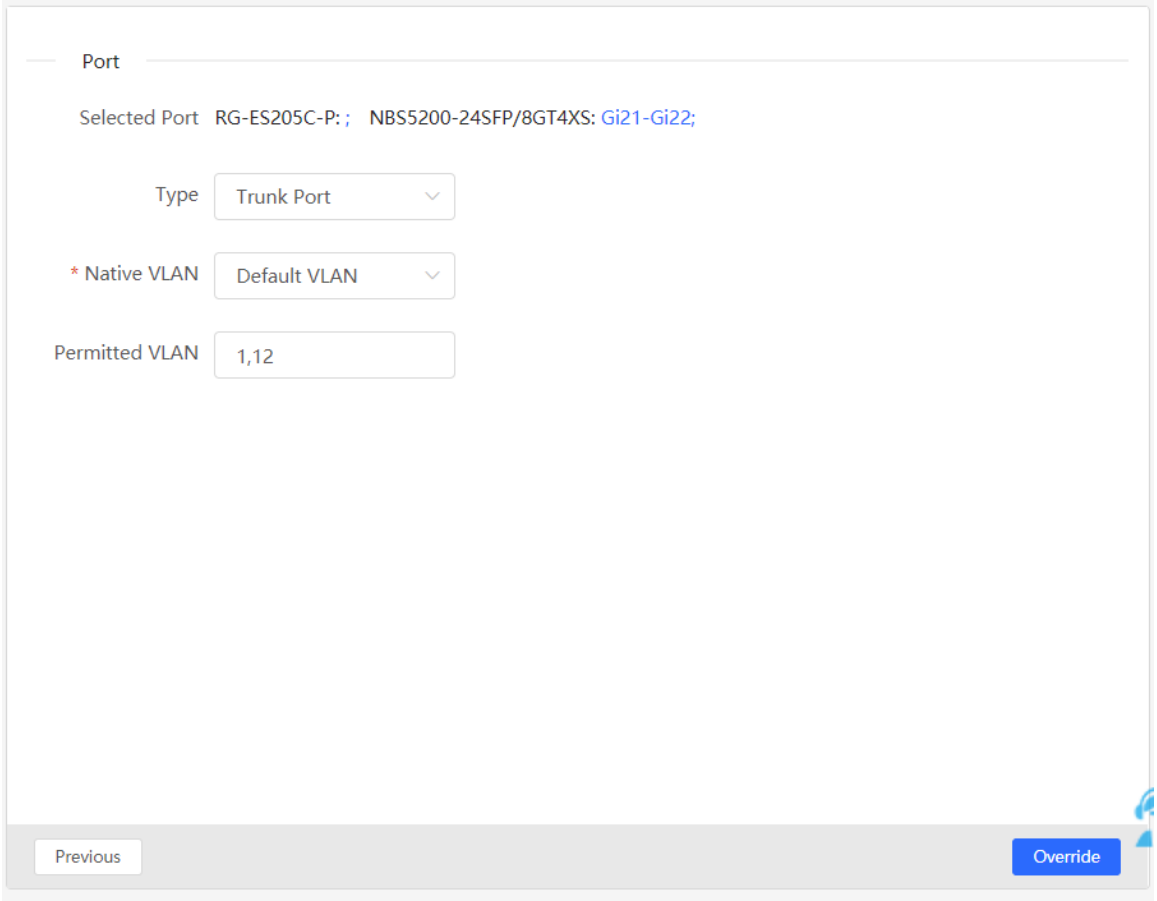
(1) The page displays all switches in the current network. Select the switches to configure, and then select the desired ports in the device port view that appears below. If there are a large number of devices in the current network, select a product model from the drop-down list box to filter the devices.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



(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**.

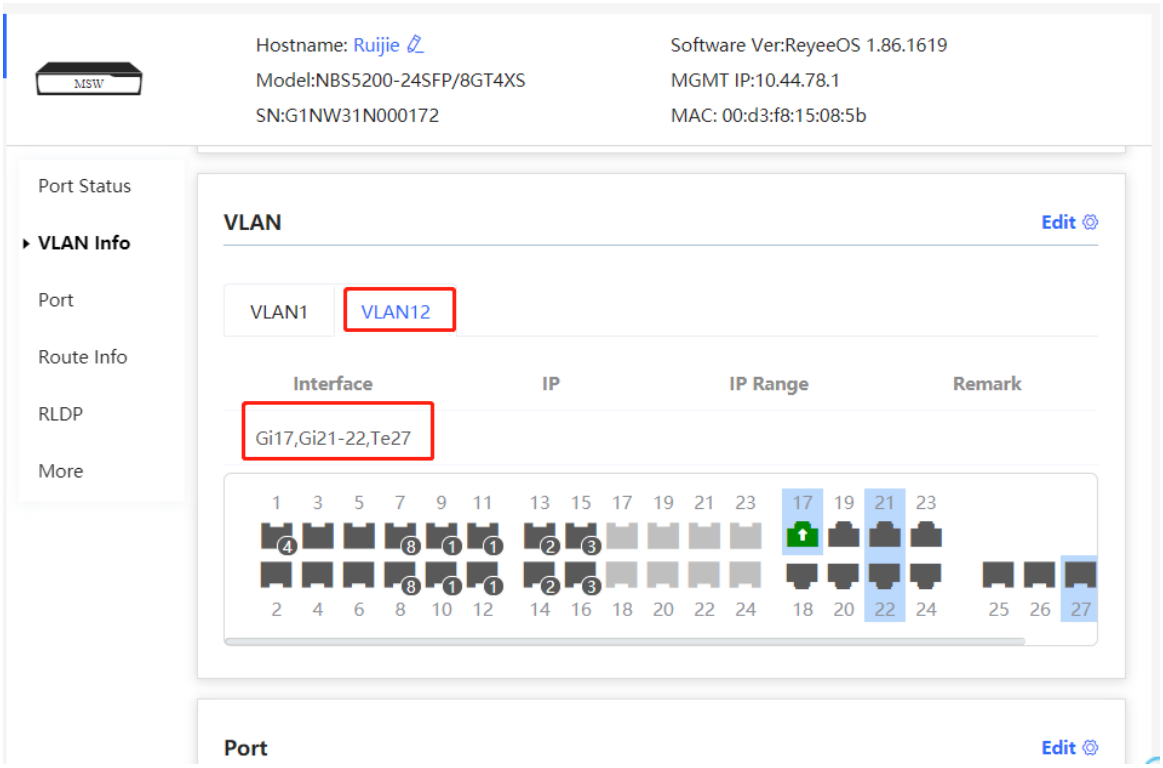


(3) Configure port attributes for the ports selected in Step 1 in a batch. Select a port type. If you set **Type** to **Access Port**, you need to configure **VLAN ID**. If you set **Type** to **Trunk Port**, you need to configure **Native VLAN** and **Permitted VLAN**. After setting the port attributes,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



3.5.5 Verifying Configuration

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



4 Port Management

4.1 Overview

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

Table 4-1 Description of Port Type

Port Type	Note	Remarks

Switch Port	A switch port consists of a single physical port on the device and provides only the L2 switching function. Switch ports are used to manage physical port and their associated L2 protocols.	Described in this section

Port Type	Note	Remarks
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

Port Type	Note	Remarks
SVI Port	A switch virtual interface (SVI) serves as the management interface of the device, through which the device can be managed. You can also create an SVI as a gateway interface, which is equivalent to the virtual interface of corresponding VLAN and can be used for inter-VLAN routing on L3 devices.	For related configuration, see 6.1

Port Type	Note	Remarks
Routed Port	On L3 devices, you can configure a single physical port as a routed port and use it as the gateway interface of L3 switching. Route interfaces do not have L2 switching functions and have no corresponding relationship with VLANs, but only serve as access interfaces.	For related configuration, see 6.1
L3 Aggregate Port	An L3 aggregate port is a logical aggregate port group composed of multiple physical member ports, just like an L2 aggregate port. The ports to be aggregated must be L3 ports of the same type. An aggregate port serves as the gateway interface of L3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections. L3 aggregate ports do not support the L2 switching function.	For related configuration, see 6.1

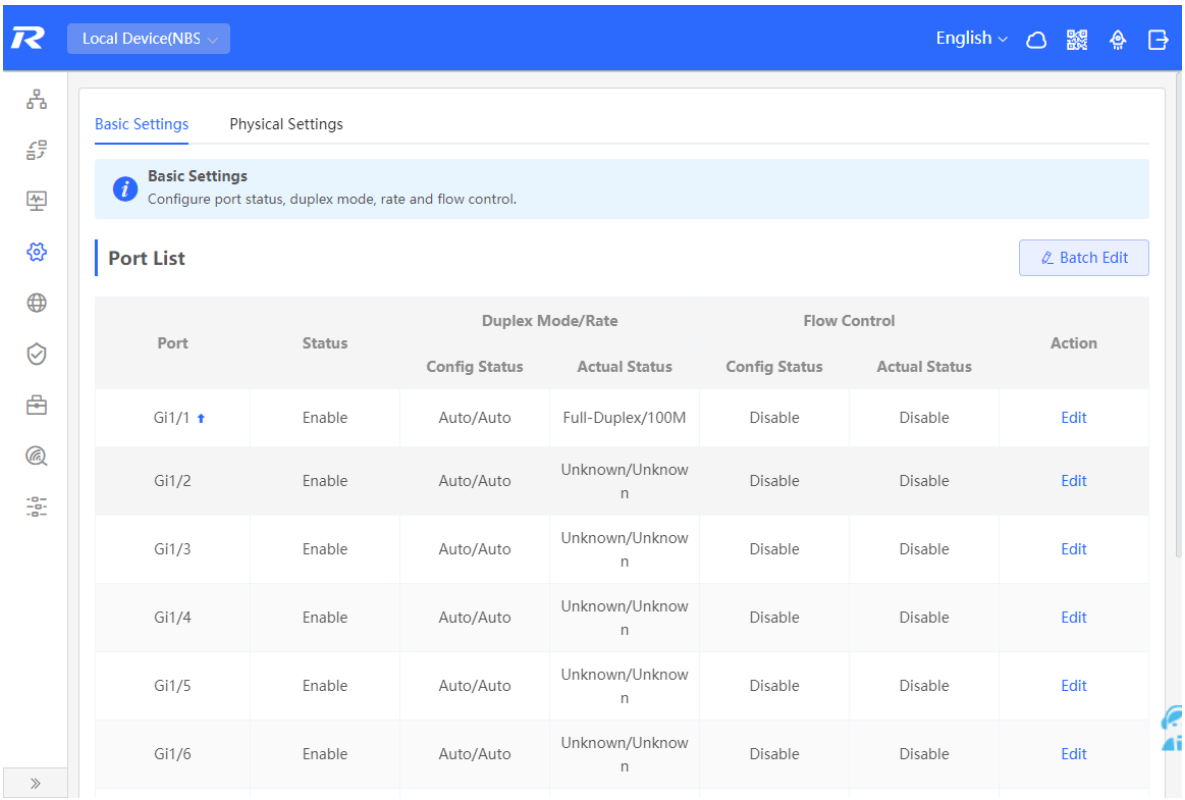
4.2 Port Configuration

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.

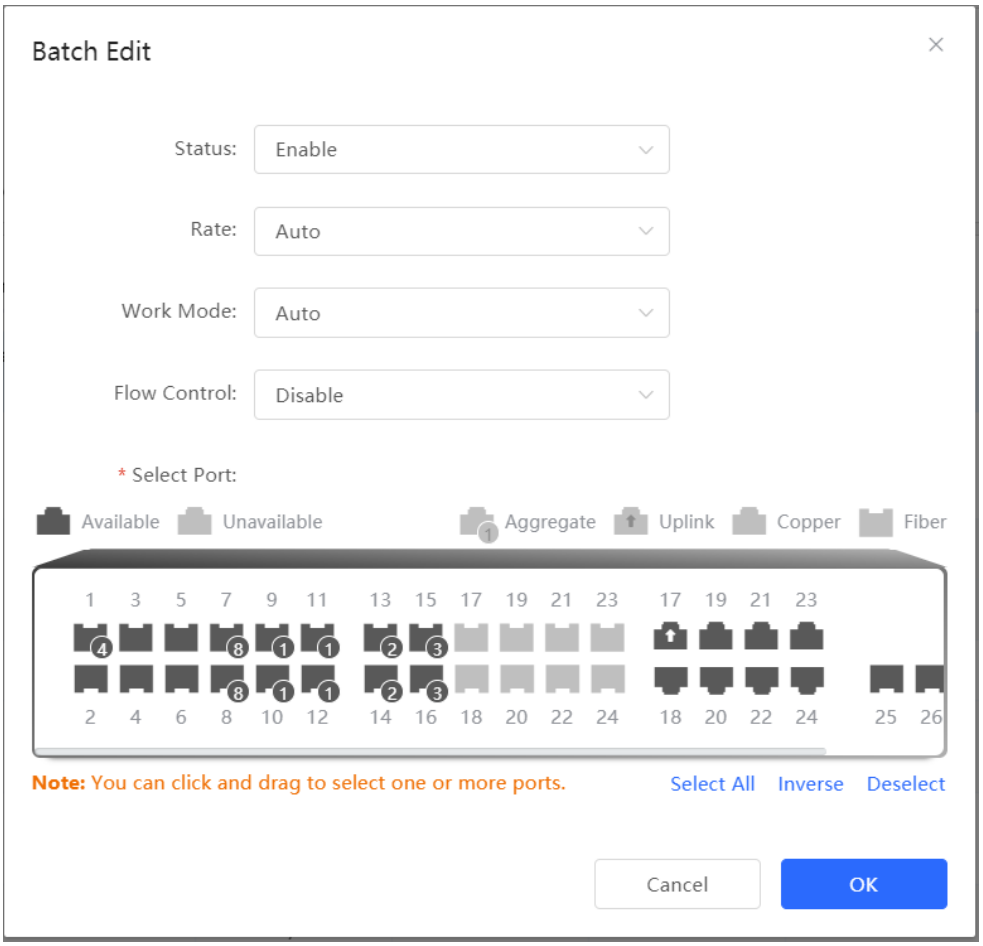
4.2.1 Basic Settings

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.



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).



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**.

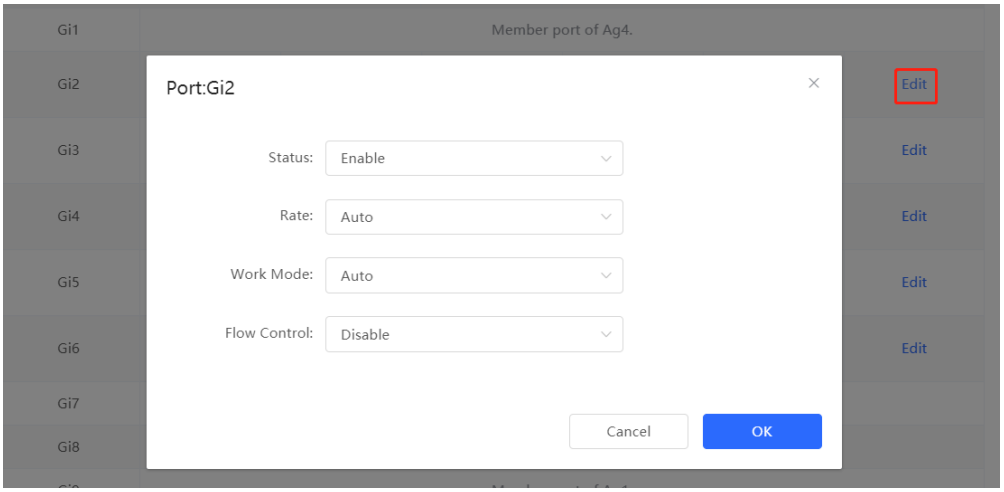


Table 4-2 Description of Basic Port Configuration Parameters

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

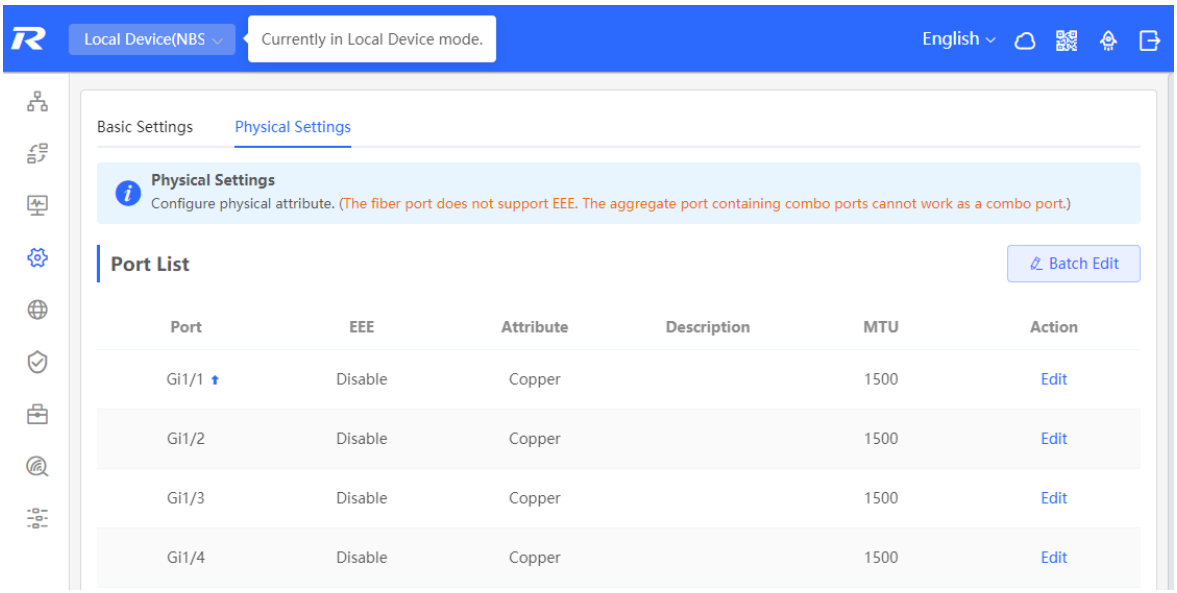
Note

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

4.2.2 Physical Settings

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

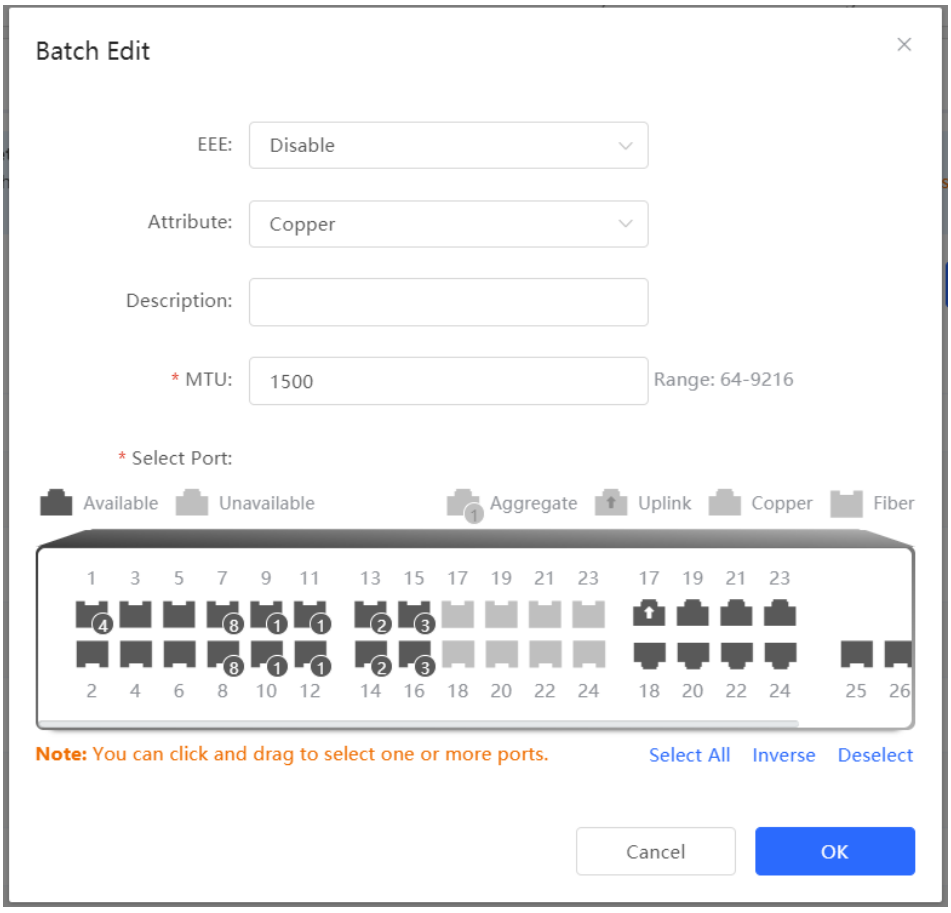
Support to enable the energy-efficient Ethernet (EEE) function of the port, and set the media type and MTU of the port.



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.



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**.

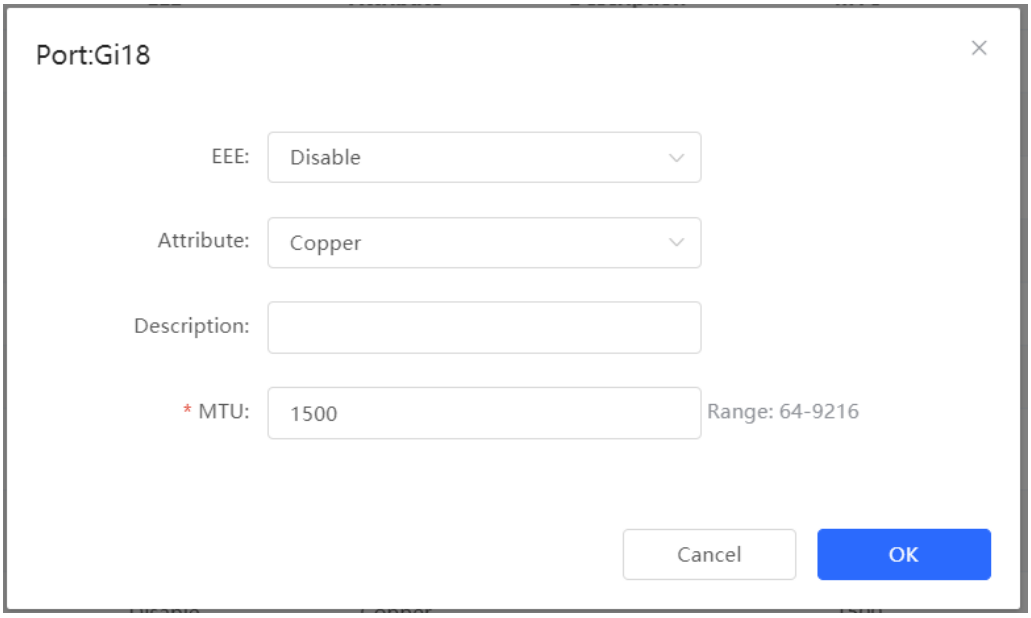


Table 4-3 Description of Physical Configuration Parameters

Parameter	Description	Default Value
EEE	It is short for energy-efficient Ethernet, which is based on the standard IEEE 802.3az protocol. When enabled, EEE saves energy by making the interface enter LPI (Low Power Idle) mode when the Ethernet connection is idle. Value: Disable/Enable	Disable
Attribute	The port attribute indicates whether the port is a copper port or an SFP port. Coper port: copper mode (cannot be changed); SFP port: fiber mode (cannot be changed); Only combo ports support mode change.	Depending on the port attribute
Description	You can add a description to label the functions of a port.	NA
MTU	MTU (Maximum Transmission Unit) is used to notify the peer of the acceptable maximum size of a data service unit. It indicates the size of the payload acceptable to the sender.. You can configure the MTU of a port to limit the length of a frame that	1500

Parameter	Description	Default Value
	can be received or forwarded through this port.	

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.

4.3 Aggregate Ports

4.3.1 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.

4.3.2 Overview

1. Static AP Address

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

2. Dynamic Aggregation

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

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

Note

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

3. Load Balancing

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

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

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Source port
- L4 source port or L4 destination port
- L4 source port + L4 destination port

4.3.3 Aggregate Port Configuration

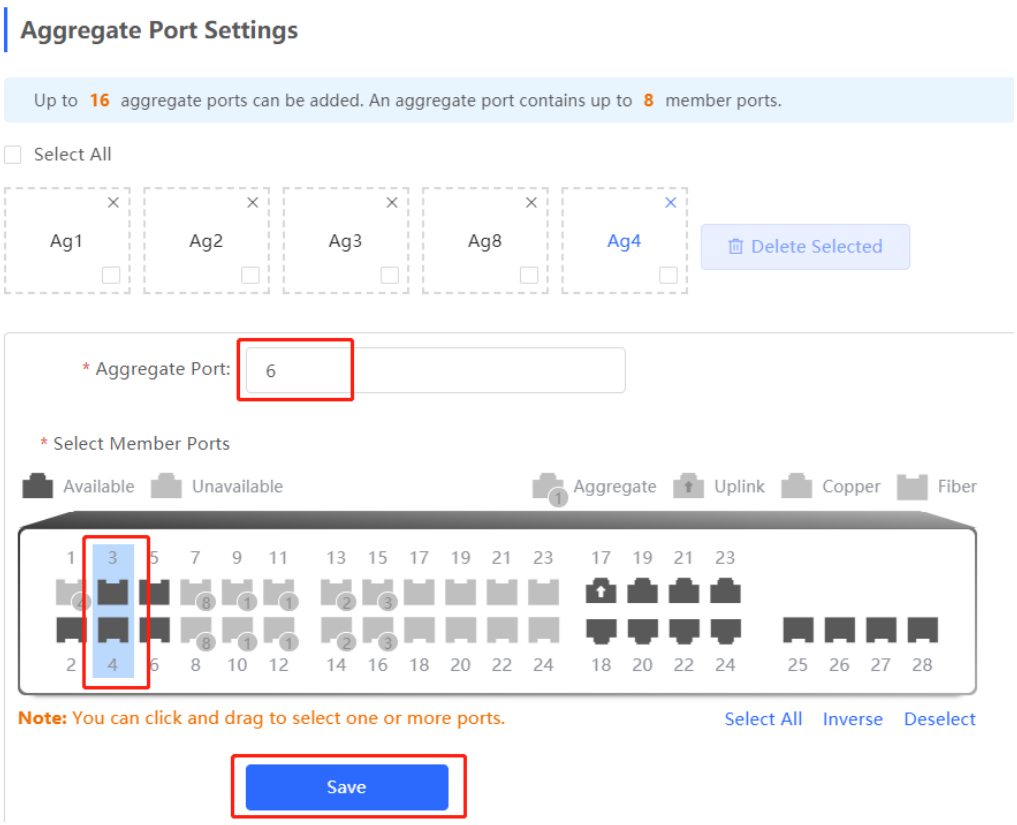
Choose **Local Device** > **Ports** > **Aggregate Ports** > **Aggregate Port Settings**.

1. Adding a Static Aggregate Port

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

Note

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

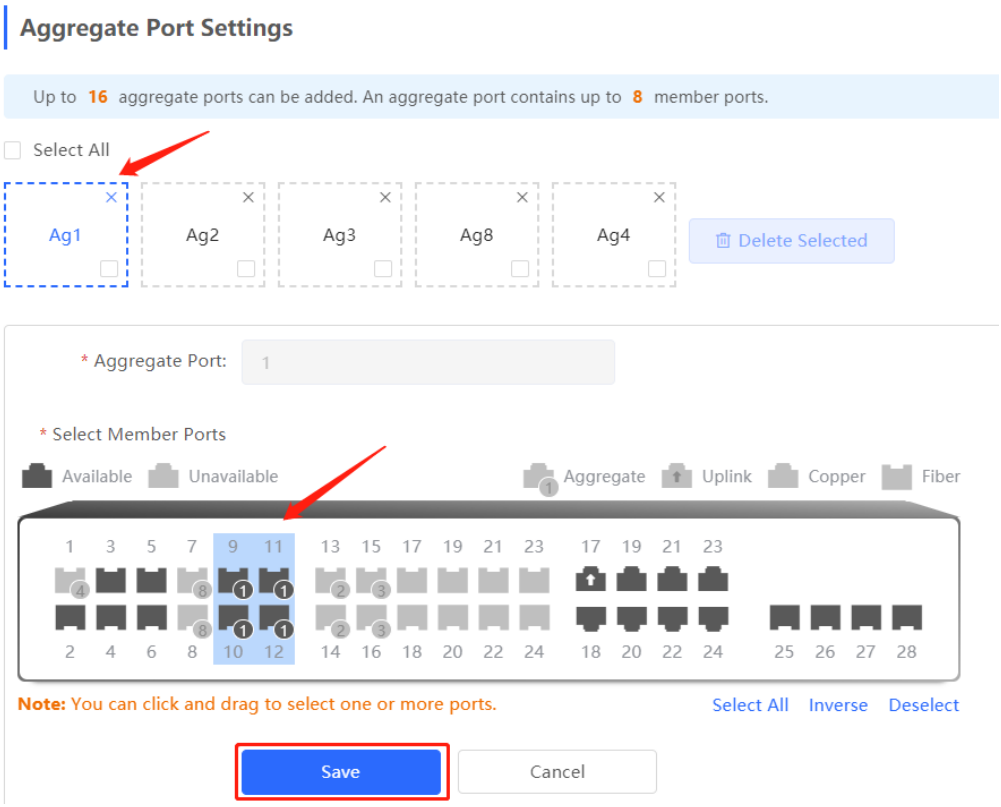


2. Modifying Member Ports of a Static Aggregate Port

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.

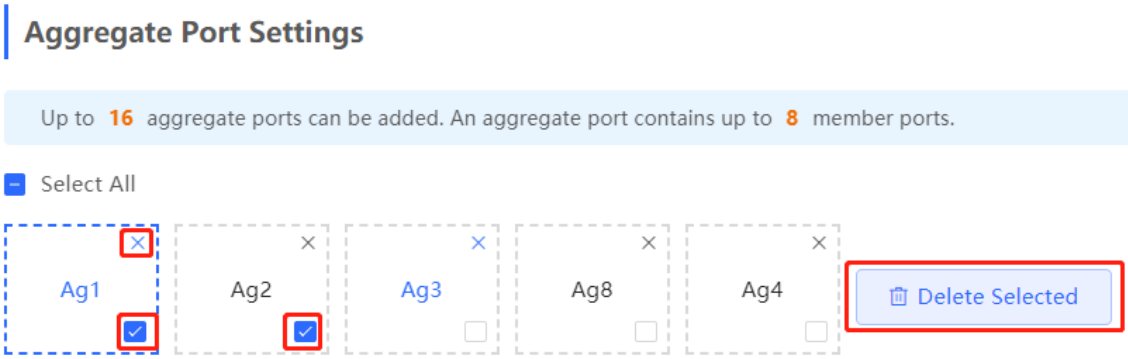


3. Deleting an Aggregate Port

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

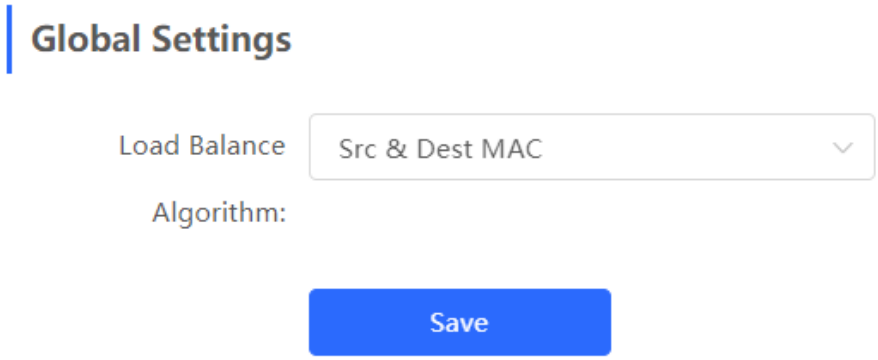
After an aggregate port is deleted, its member ports are restored to the default settings and are disabled.



4.3.4 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.



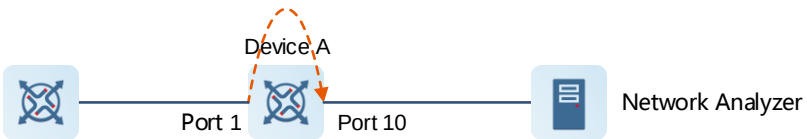
4.4 Port Mirroring

4.4.1 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 4-1 Port Mirroring Principles Figure



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

4.4.2 Procedure

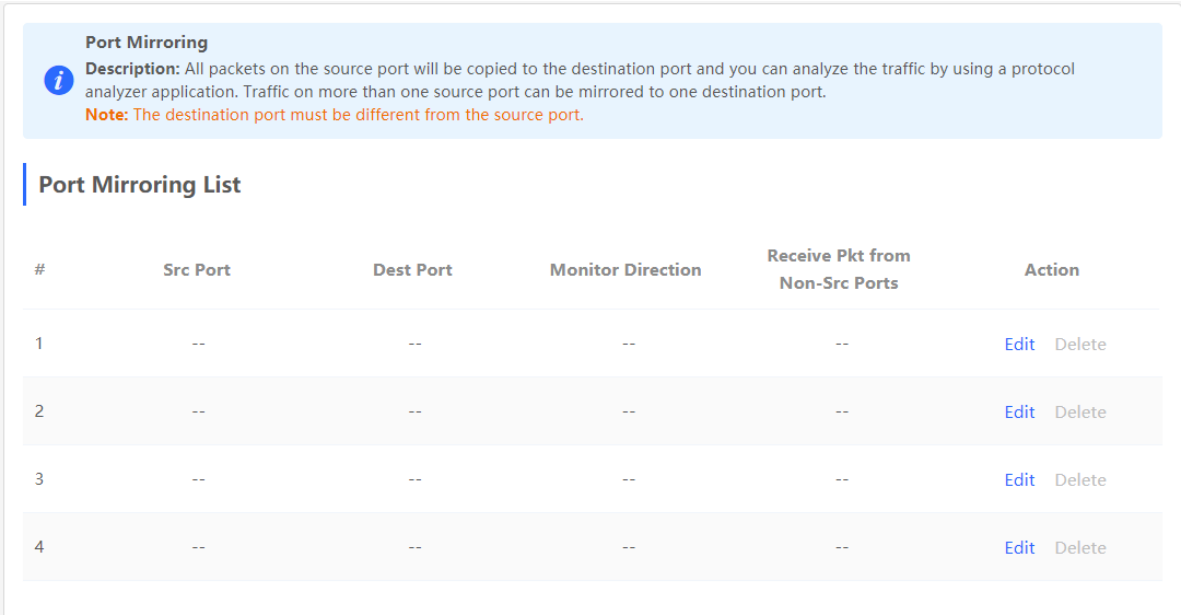
Choose **Local Device** > **Ports** > **Port Mirroring**.

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

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

Caution

- You can select multiple source traffic monitoring ports but only one destination port. Moreover, the source traffic monitoring ports cannot contain the destination port.
- An aggregate port cannot be used as the destination port.
- A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.



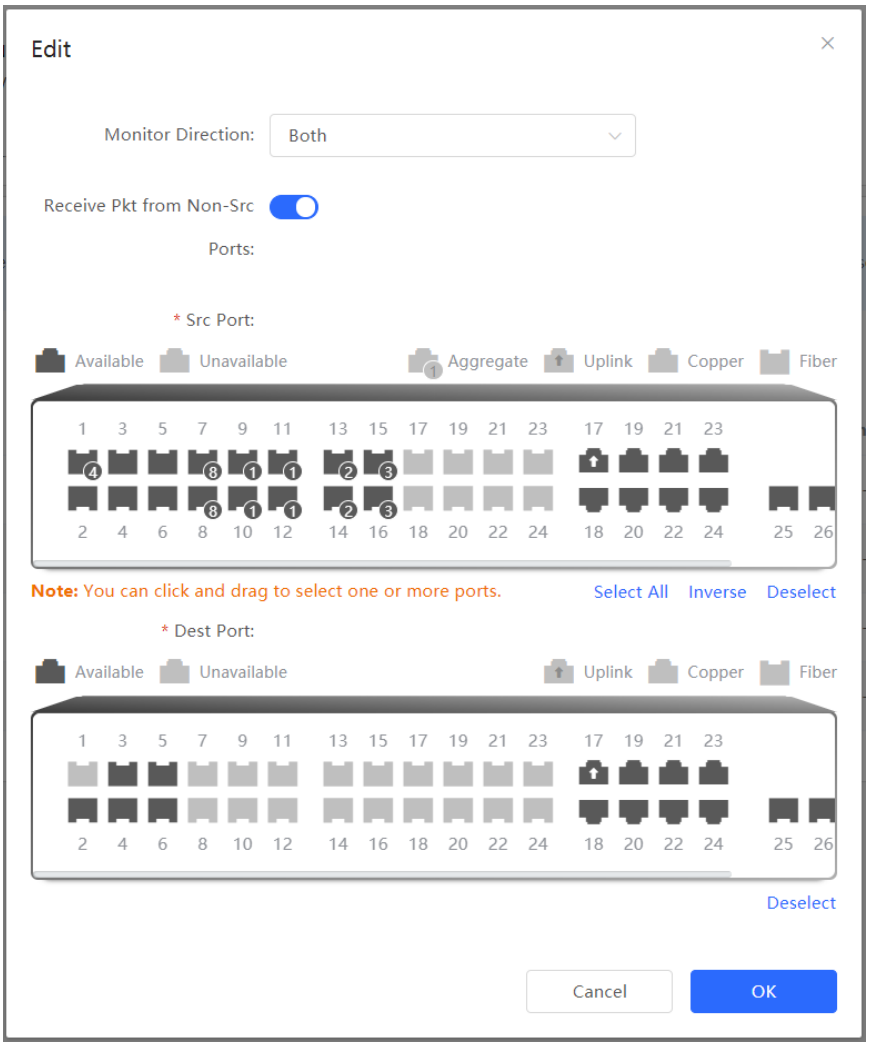


Table 4-4 Description of Port Mirroring Parameters

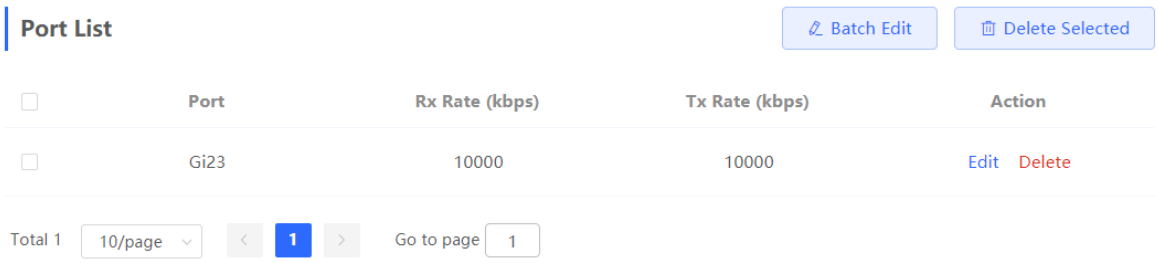
Parameter	Description	Default Value
Src Port	A source port is also called a monitored port. Data flows on the source port are monitored for network analysis or troubleshooting. Support selecting multiple source ports and mirroring multiple ports to one destination port	N/A
Dest Port	The destination port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

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 ● Outcoming: All packets transmitted by a source port are copied to the destination port	Both
Receive Pkt from Non-Src Ports	It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets. ● Enabled: While monitoring the packets of the source port, the packets of other non-Src ports are normally forwarded ● Disabled: Only monitor source port packets	Enable

4.5 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.



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.

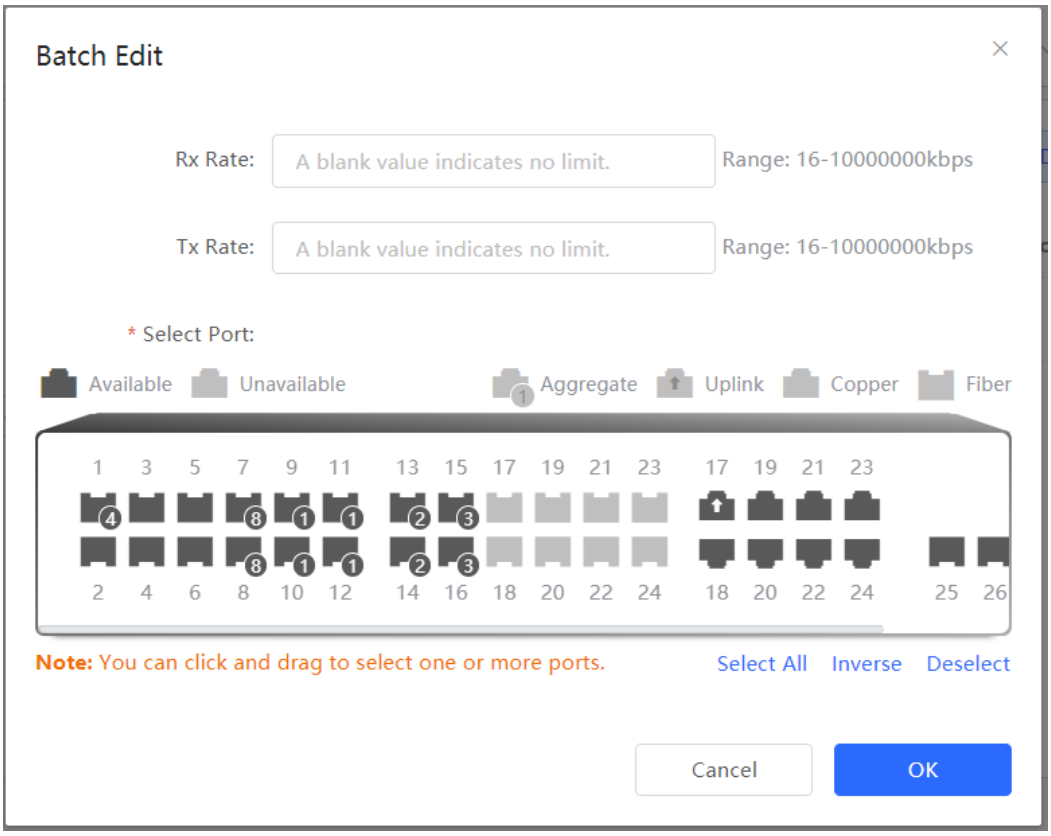
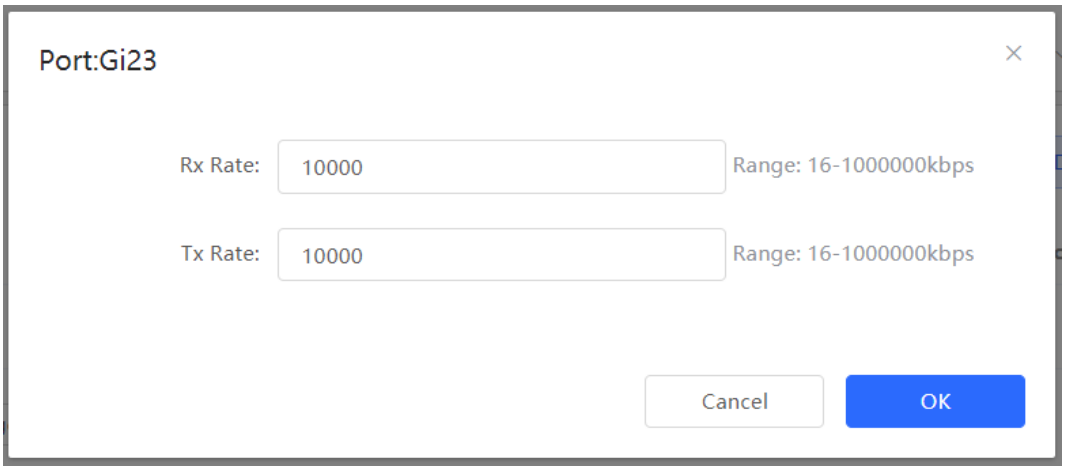


Table 4-5 Description of Rate Limiting Parameters

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

2. Changing Rate Limits of a Single Port

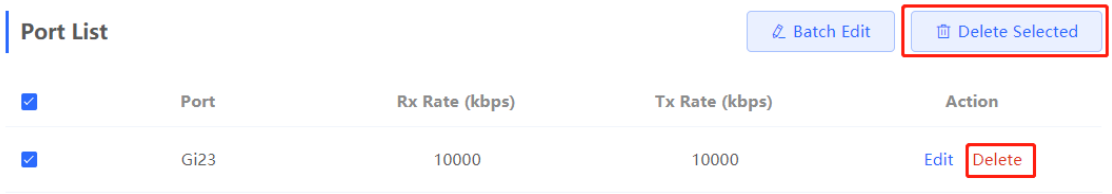
In the port list for which the rate limit has been set, click **Edit** on the corresponding port entry, enter the ingress rate and egress rate in the displayed dialog box, and click **OK**.



3. Deleting Rate Limiting

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

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



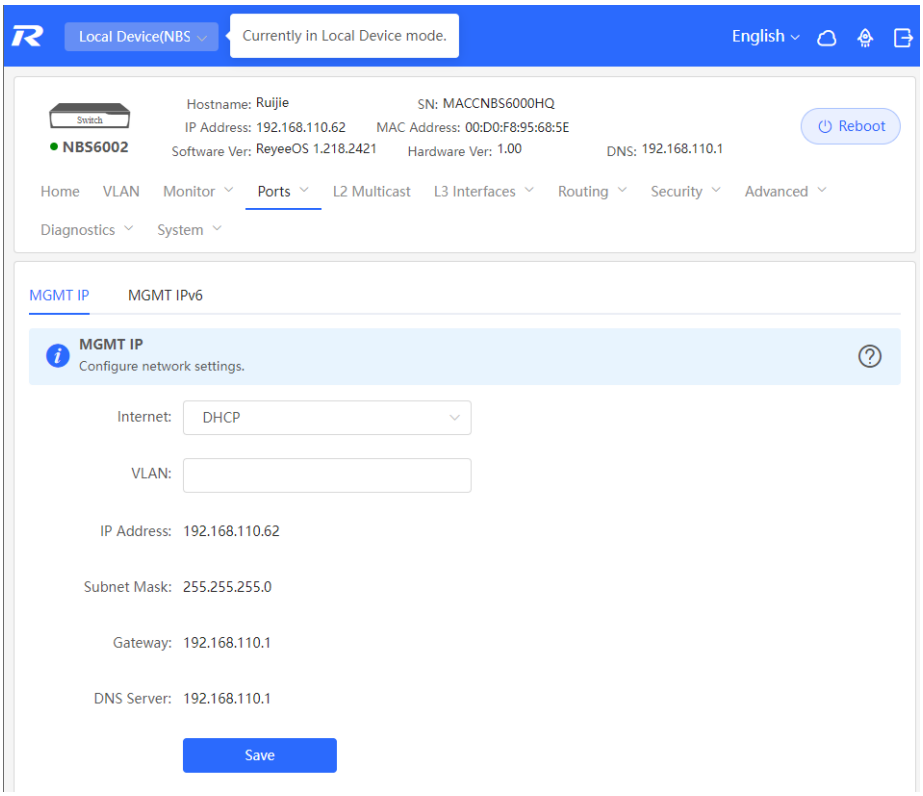
Note

- 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.

4.6 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.



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 3.5.2).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the Eweb management system.

4.7 Configuring the Management IPv6 Address

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

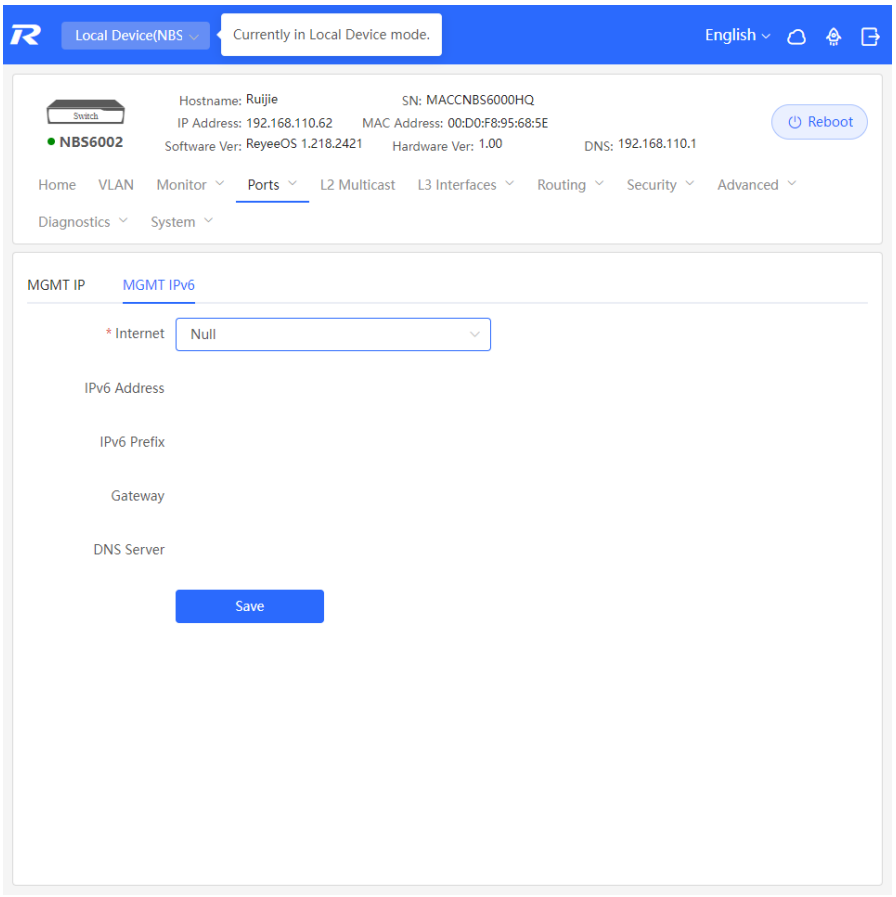
Choose **Local Device** > **Ports** > **MGMT IP** > **MGMT IPv6**.

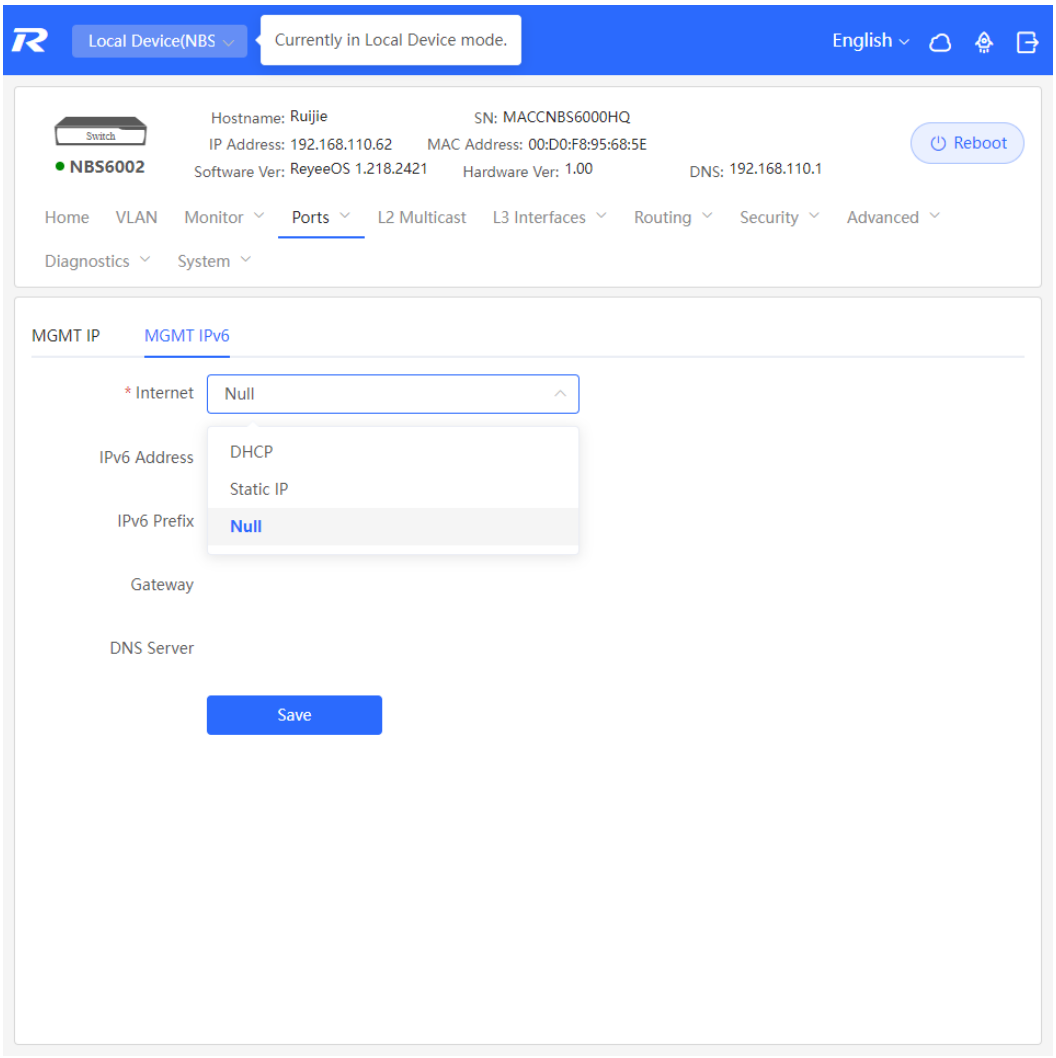
Configure the management IPv6 address so that you can log in to the device management page using the IPv6 address of the device.

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**.





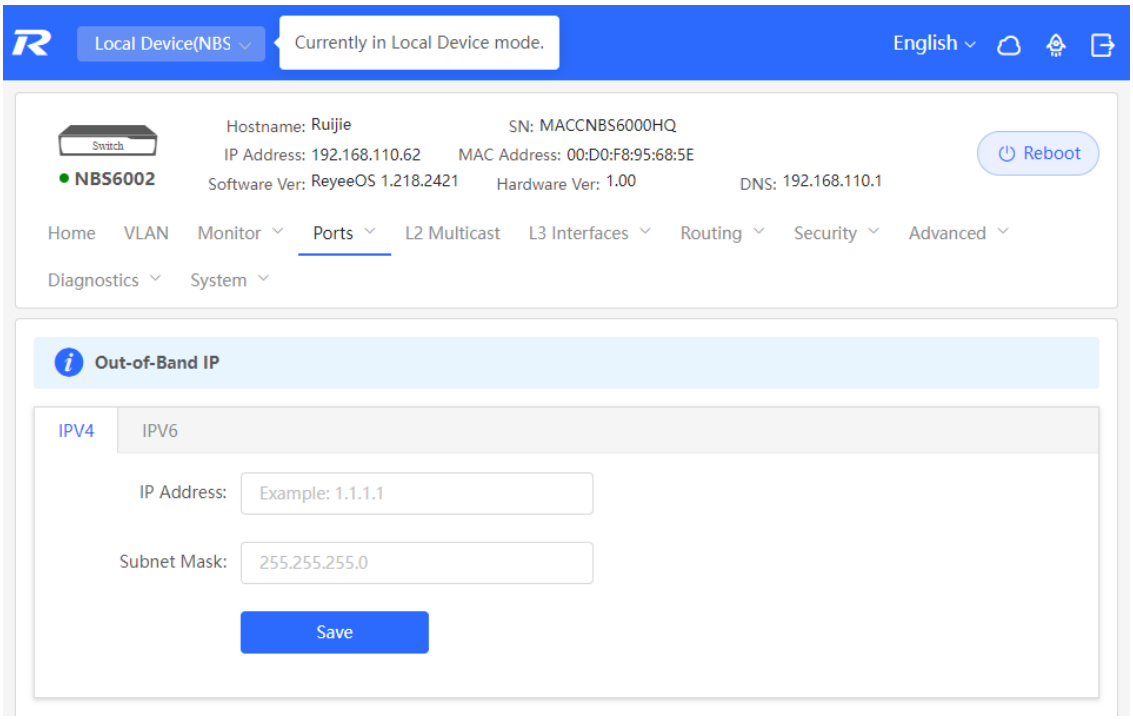
4.8 Out-of-Band IP Configuration

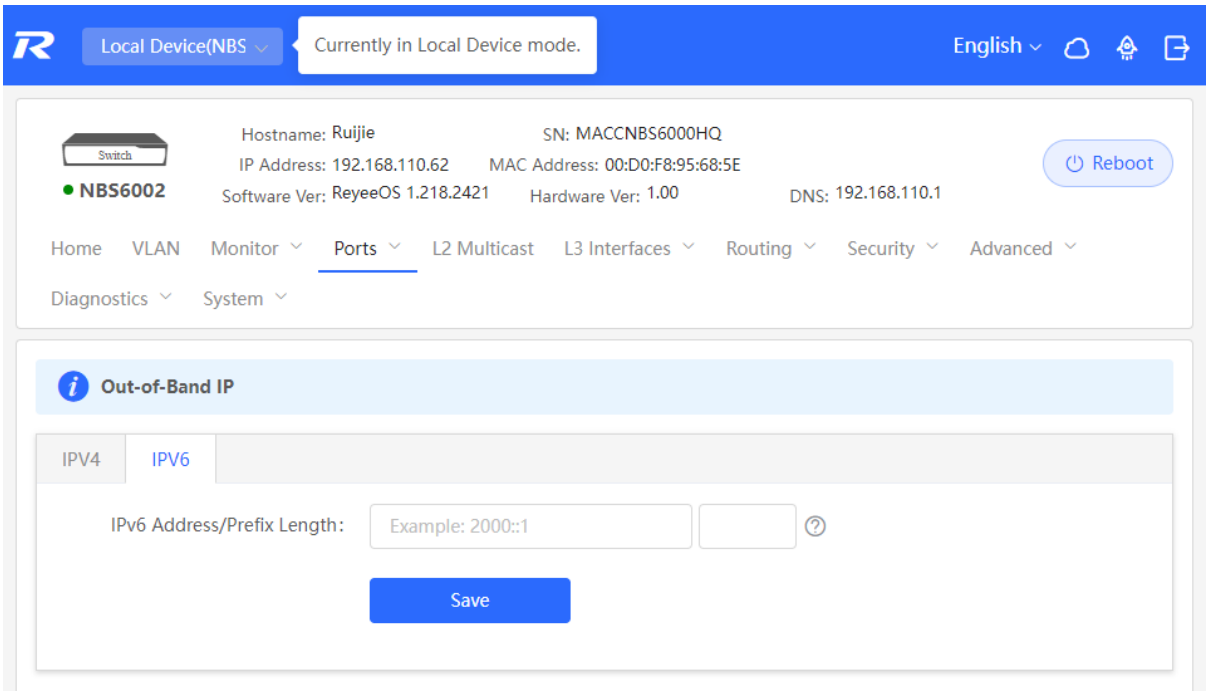
Caution

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

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

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





Note

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

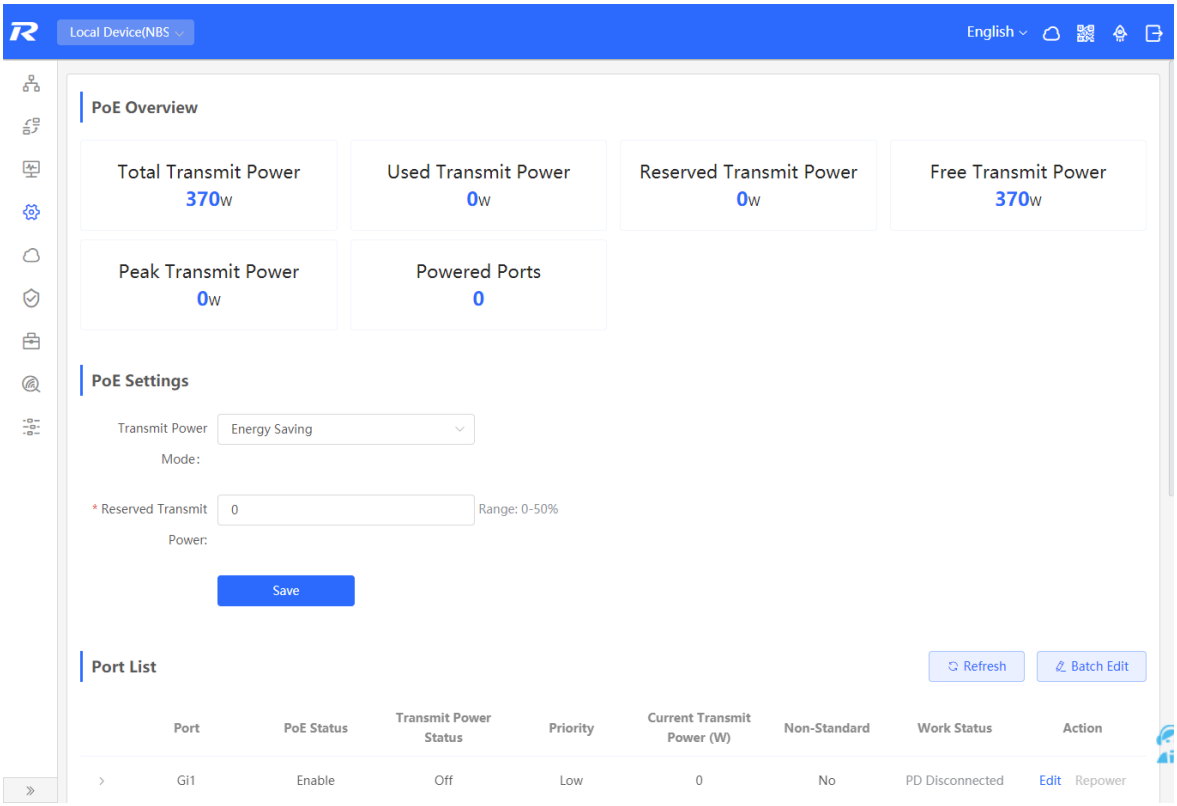
4.9 PoE Configuration

Caution

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

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

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



4.9.1 PoE Global Settings

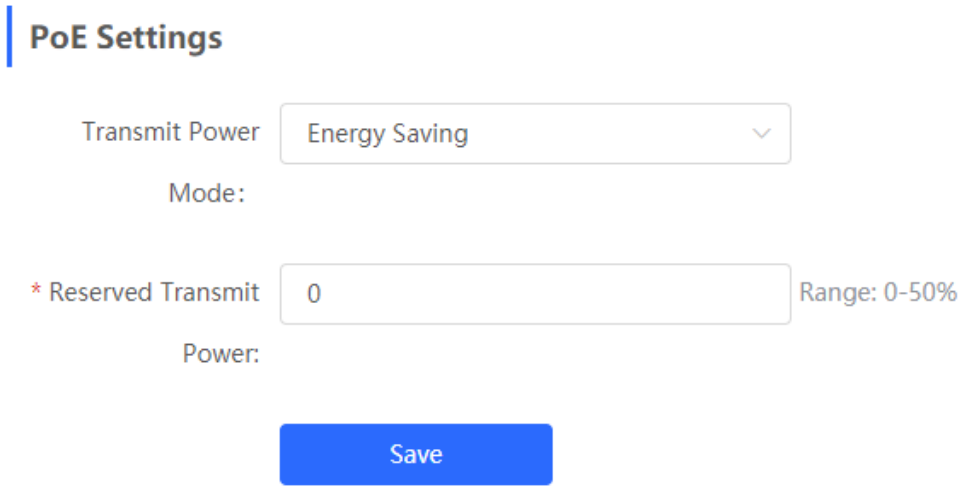
Choose **Local Device** > **Ports** > **PoE** > **PoE Settings**.

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.

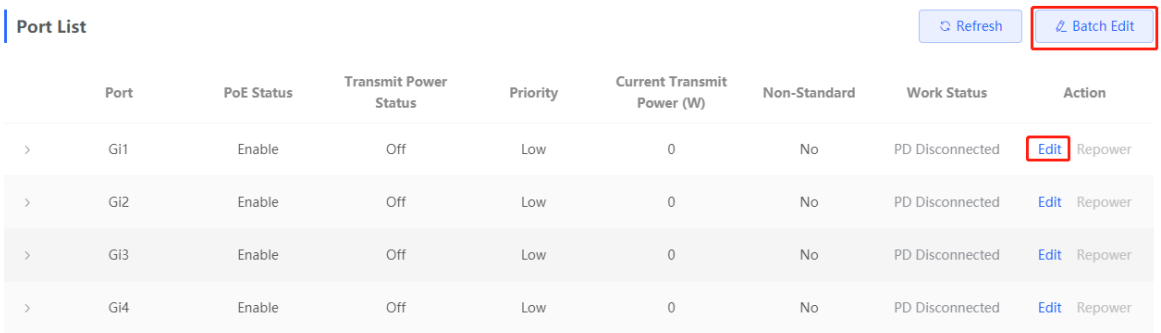
In energy-saving mode, the PoE device dynamically adjusts allocated power based on actual consumption of PDs. In this mode, in order to prevent the power supply of the port from fluctuating due to the fluctuation of the actual power consumption of the PD when the power is fully loaded, you can set the 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.



4.9.2 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.



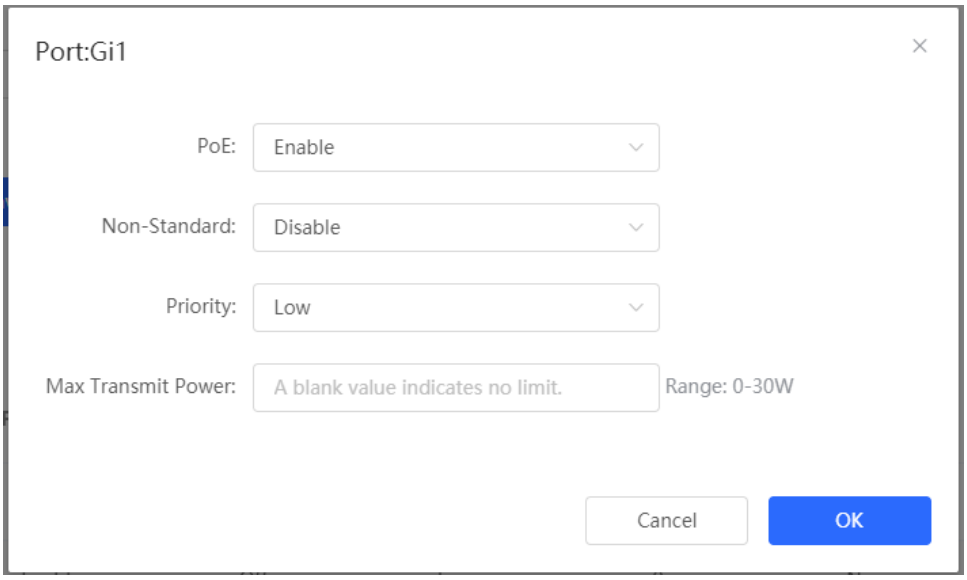


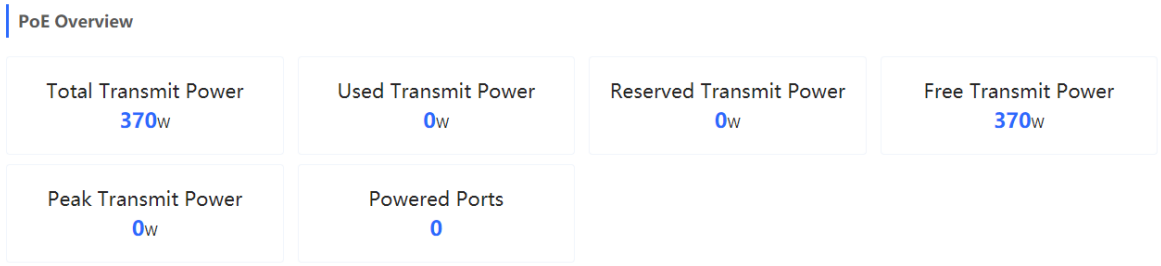
Table 4-6 Description of Parameters for Power Supply Configuration of Ports

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

4.9.3 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.



4.9.4 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.

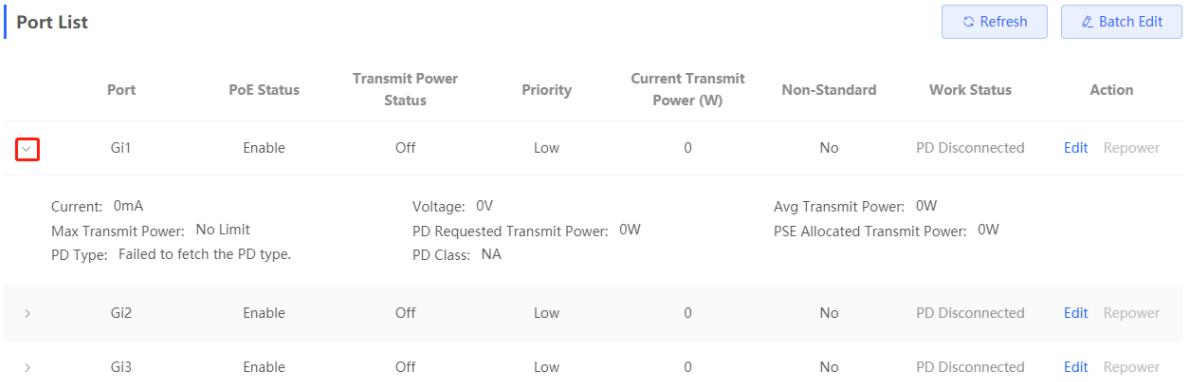


Table 4-7 Description of Port Power Supply Info

Field	Description
Port	Device Port ID
PoE Status	Whether to enable the PoE function on the ports.
Transmit Power Status	Whether the port supplies power for Pds currently.
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low.

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

5 L2 Multicast

5.1 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.

5.2 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.

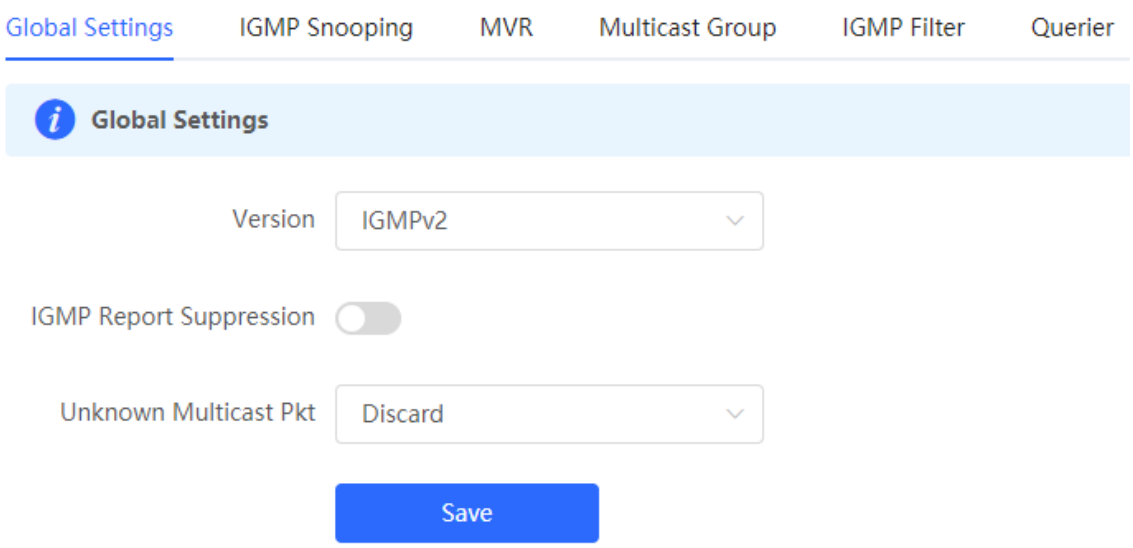


Table 5-1 Description of Configuration Parameters of Global Multicast

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

5.3 IGMP Snooping

5.3.1 Overview

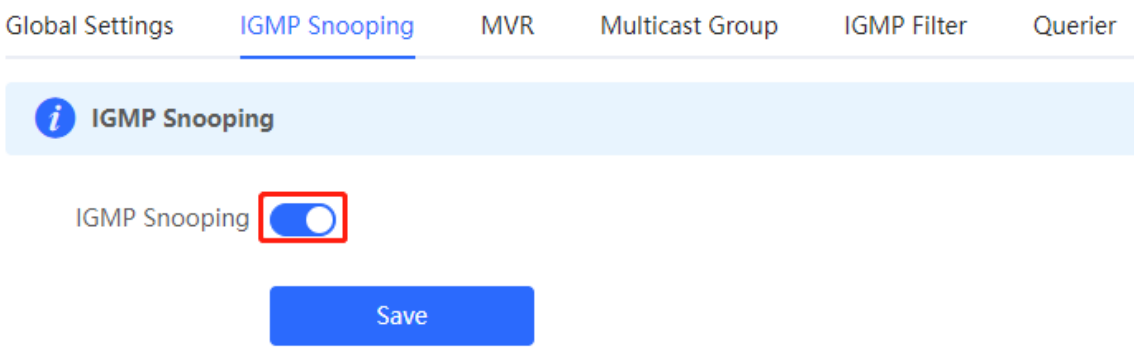
The Internet Group Management Protocol (IGMP) snooping is an IP multicast snooping mechanism running on a VLAN to manage and control the forwarding of IP multicast traffic within the VLAN. It implements the L2 multicast function.

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

5.3.2 Enabling Global IGMP Snooping

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

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



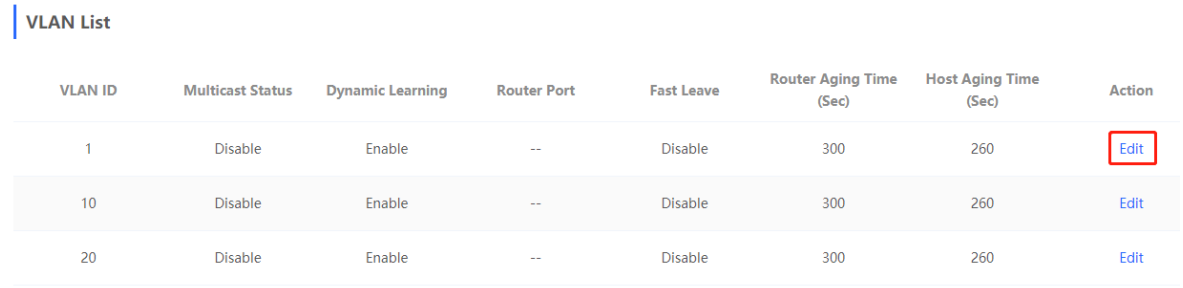
5.3.3 Configuring Protocol Packet Processing Parameters

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**.



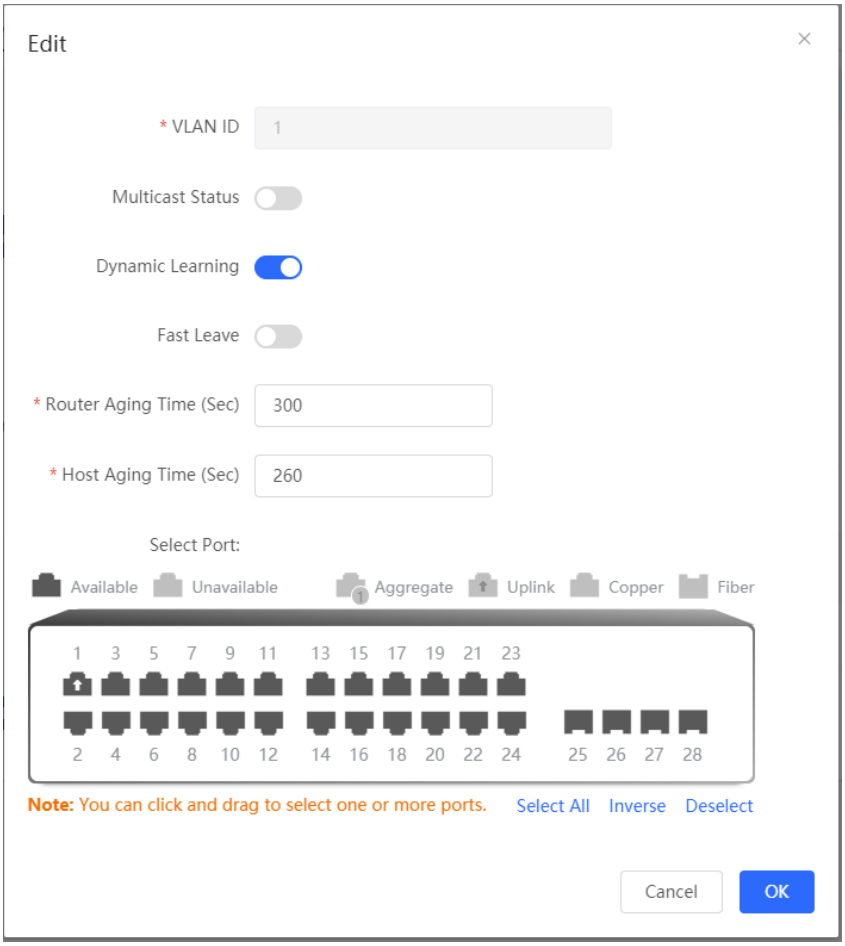


Table 5-2 Description of VLAN Configuration Parameters of IGMP Snooping

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

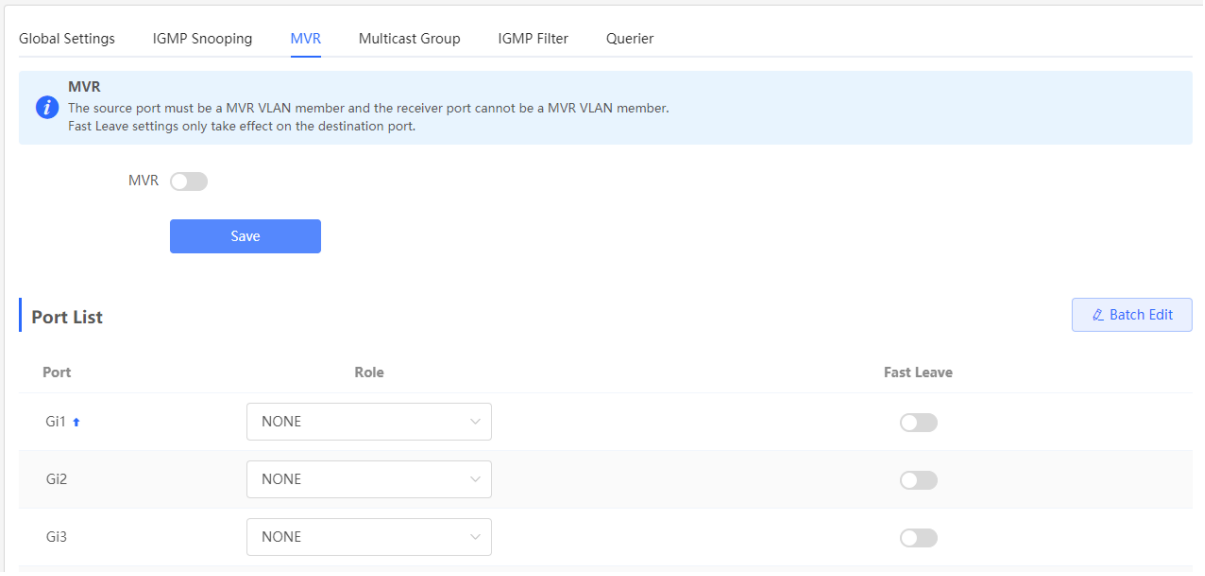
Parameter	Description	Default Value
Dynamic Learning	The device running IGMP Snooping identifies the ports in the VLAN as router ports or member ports. The router port is the port on the Layer 2 multicast device that is connected to the Layer 3 multicast device, and the member port is the host port connected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

5.4 Configuring MVR

5.4.1 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.



5.4.2 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.

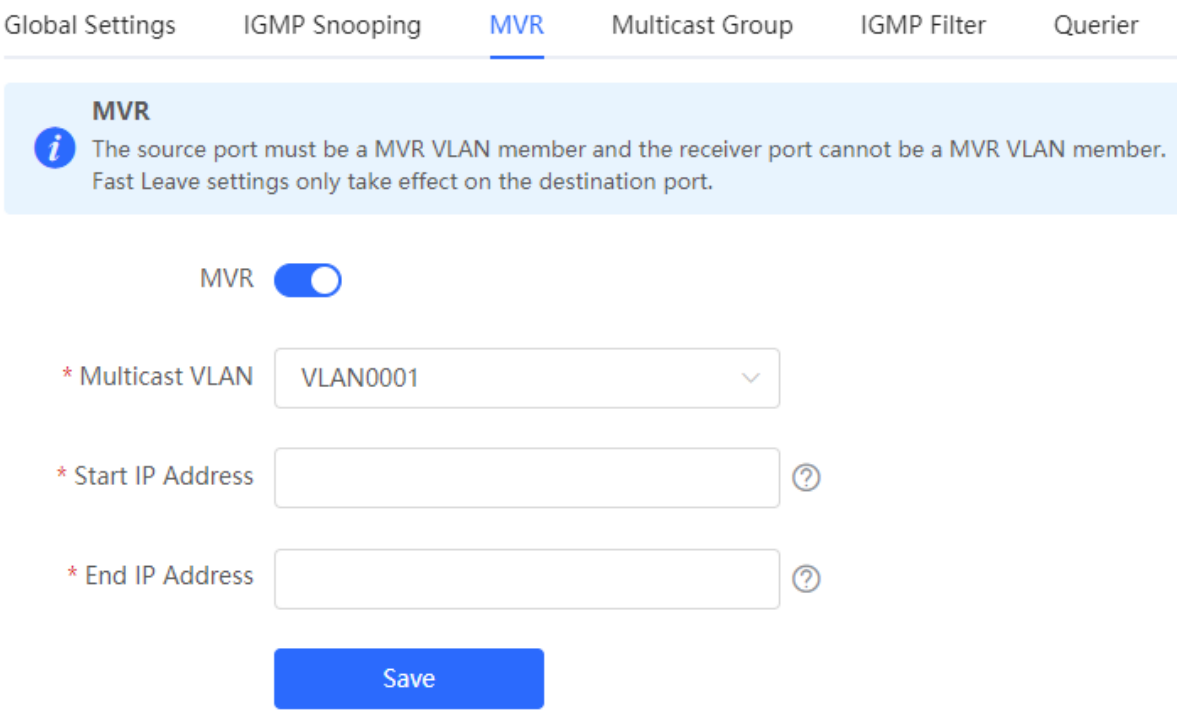


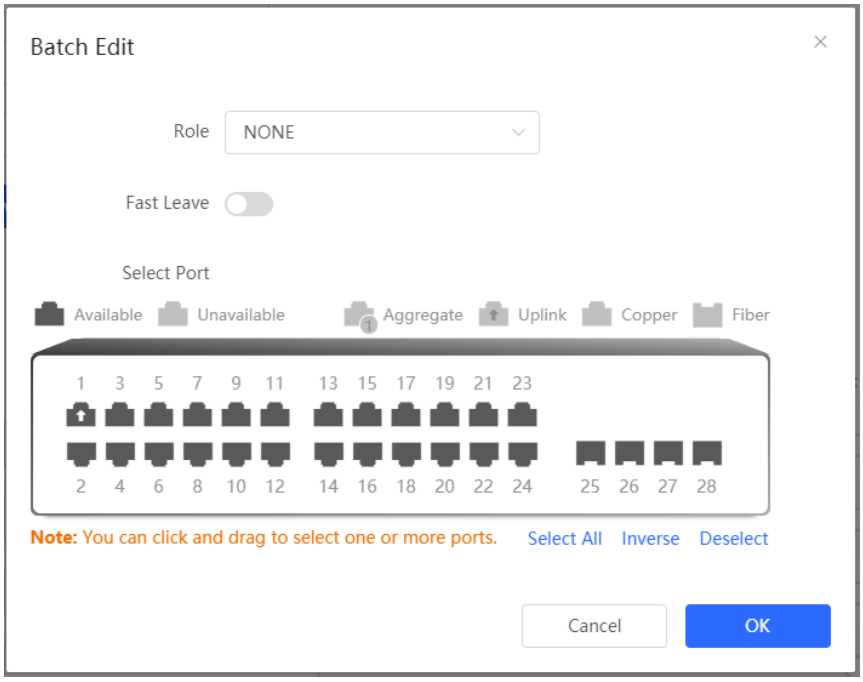
Table 5-3 Description of Configuring Global MVR Parameters

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.	NA
End IP Address	Learned or configured end multicast IP address of an MVR multicast group.	NA

5.4.3 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**.



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.

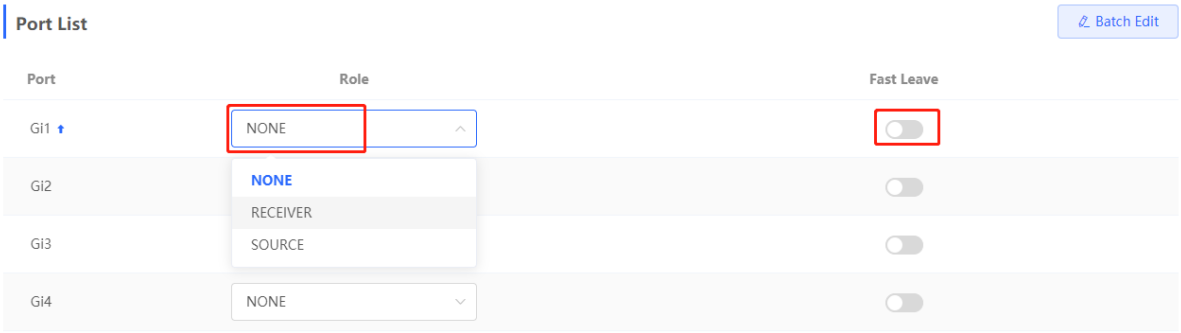


Table 5-4 Description of MVR Configuration Parameters of Ports

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

Note

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

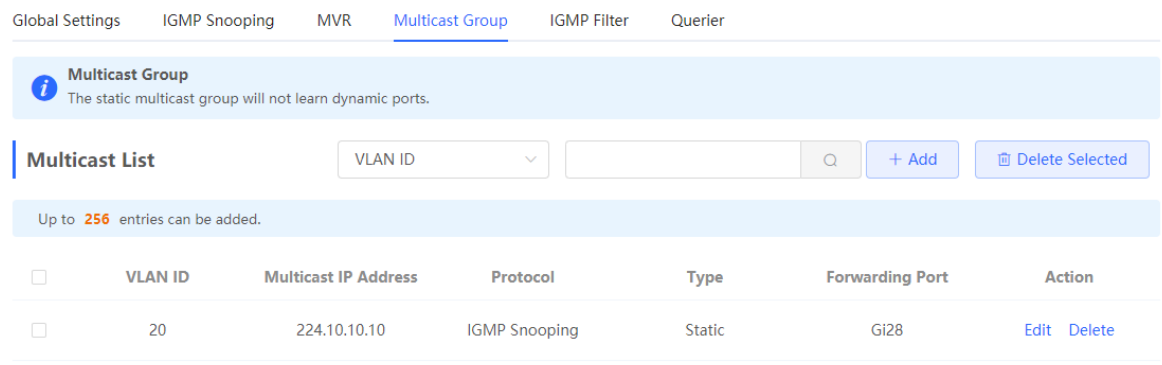
5.5 Configuring Multicast Group

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.



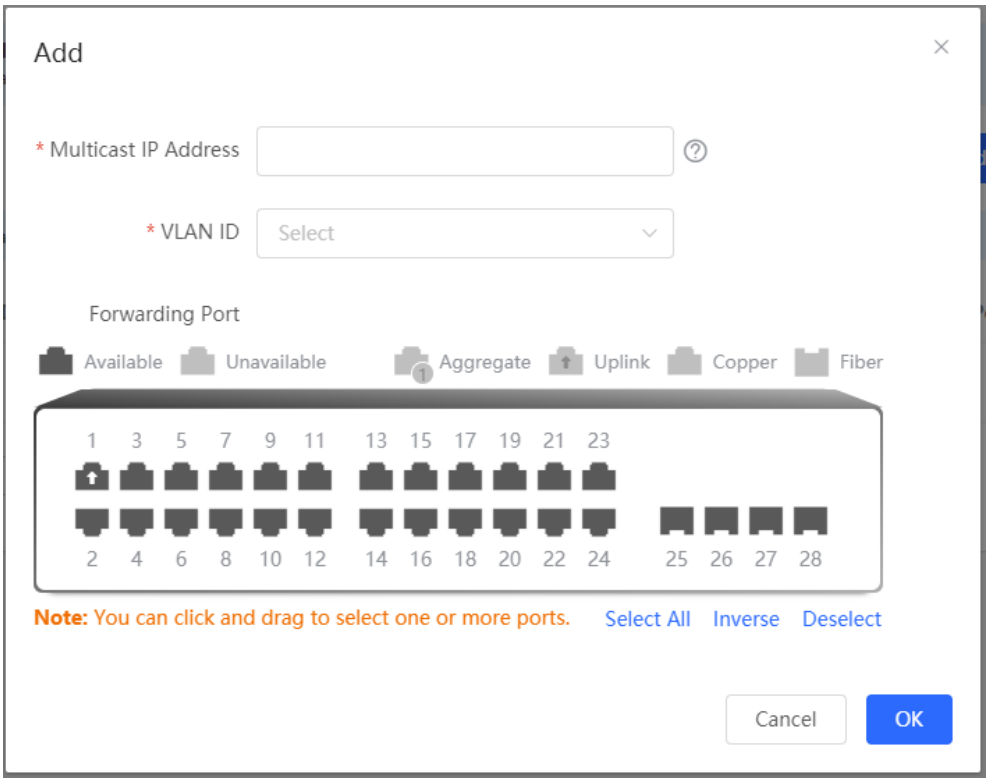


Table 5-5 Description of Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	NA
Multicast IP Address	On-demand multicast IP address	NA
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	NA

Parameter	Description	Default Value
Type	Multicast group generation mode can be statically configured or dynamically learned. In normal cases, a port can join a multicast group only after the port receives an IGMP Report packet from the multicast, that is, dynamically learned mode. If you manually add a port to a group, the port can be statically added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.	NA
Forwarding Port	List of ports that forward multicast traffic	NA

Note

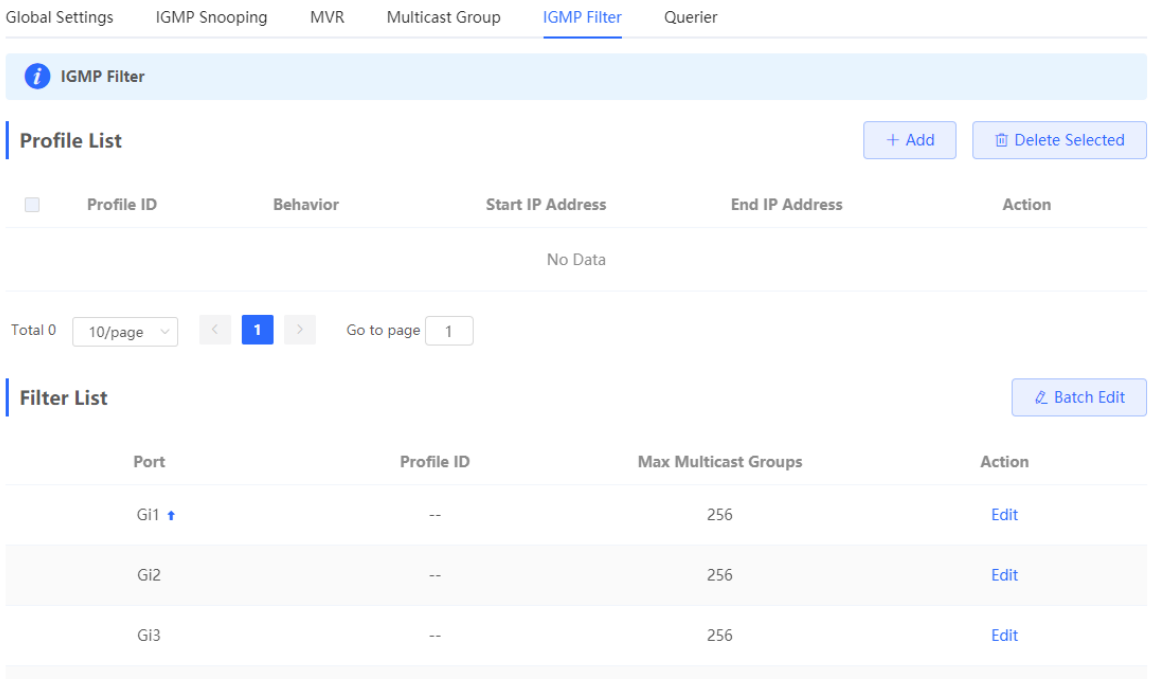
Static multicast groups cannot learn other dynamic forwarding ports.

5.6 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.



5.6.1 Configuring Profile

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

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

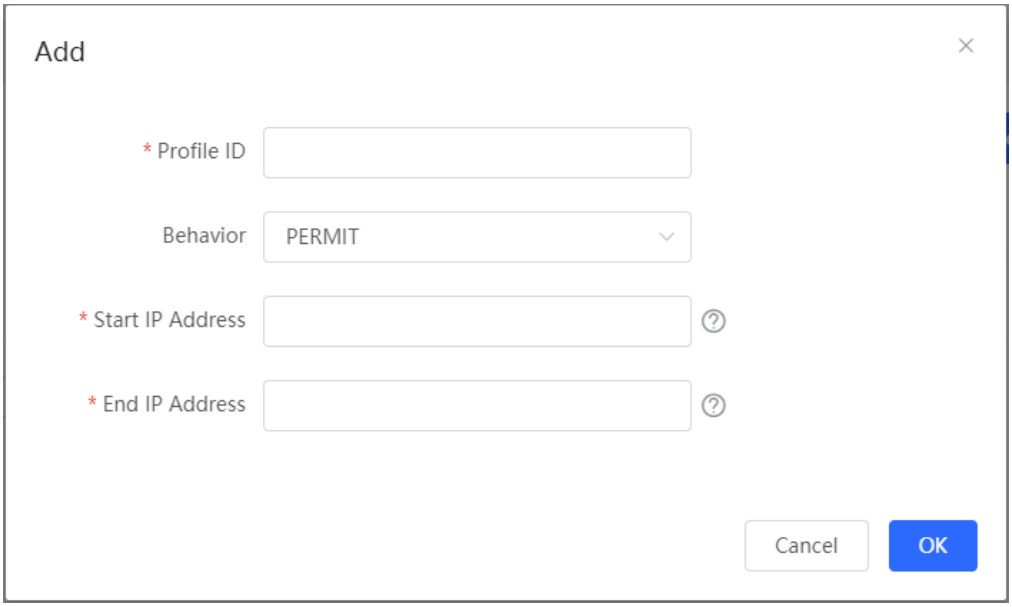


Table 5-6 Description of Profile Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile ID	NA

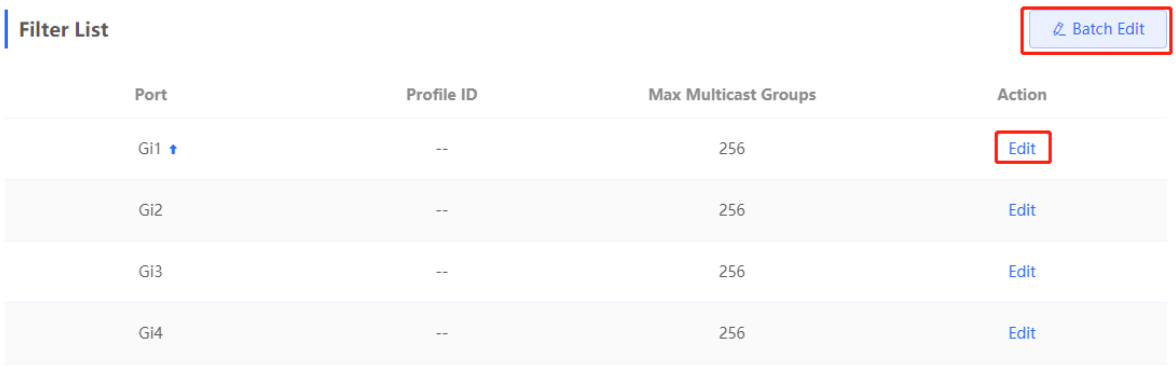
Parameter	Description	Default Value
Behavior	**DENY**: Forbids demanding multicast IP addresses in a specified range. **PERMIT**: Only allows demanding multicast IP addresses in a specified range.	NA
Start IP Address	Start Multicast IP address of the range of multicast group addresses	NA
End IP Address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

5.6.2 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**.



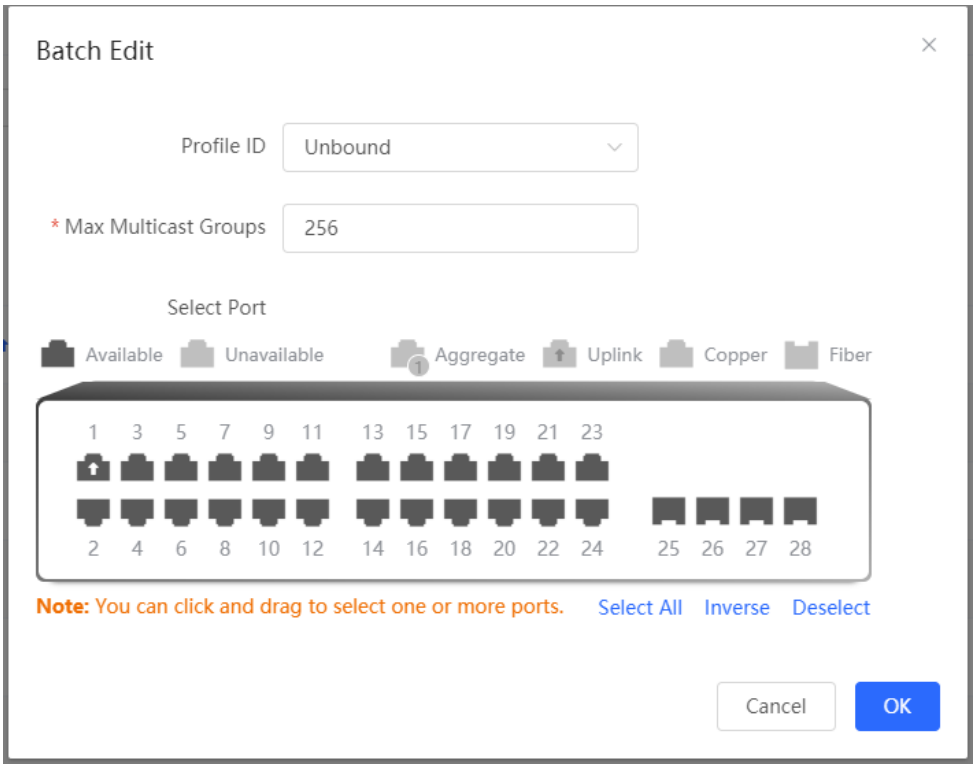


Table 5-7 Description of Port Filter Configuration Parameters

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

5.7 Setting an IGMP Querier

5.7.1 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

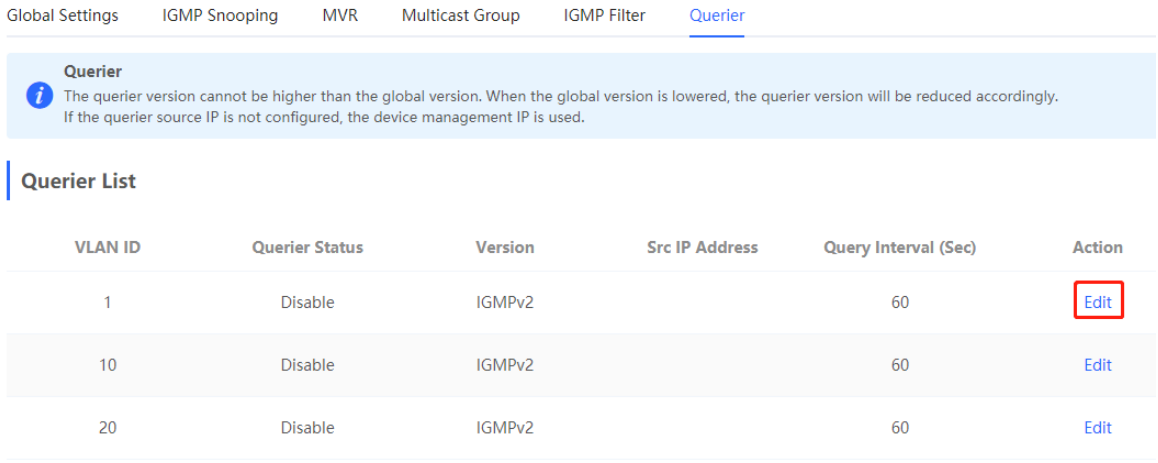
to user hosts on behalf of the L3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish L2 multicast forwarding entries.

5.7.2 Procedure

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

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

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



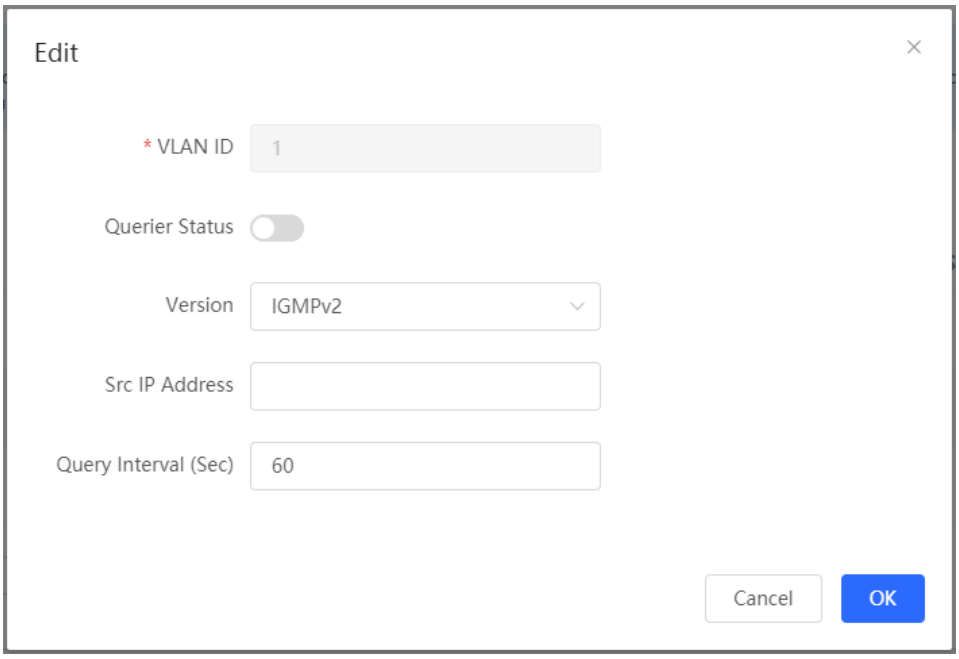


Table 5-8 Description of Querier Configuration Parameters

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

Note

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

6 L3 Management

Caution

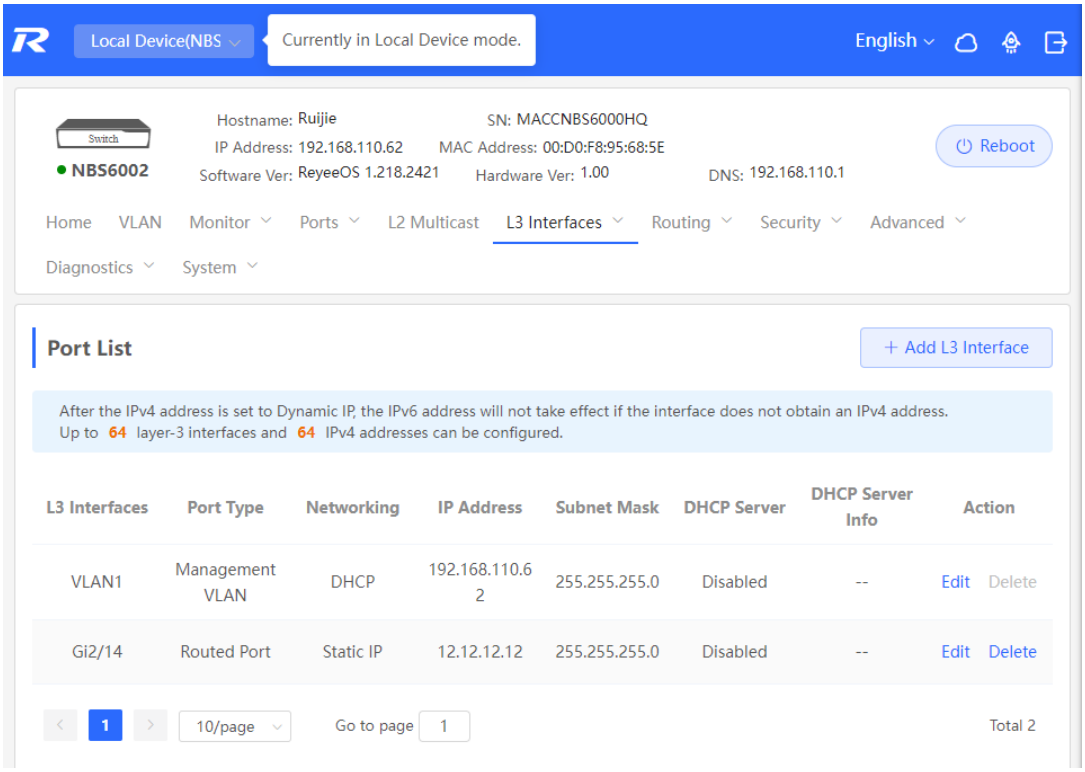
This section is applicable only to NBS Series Switches that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series Switches, RG-NBS3200 Series Switches, do not support the functions mentioned in this section.

6.1 Setting an L3 Interface

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

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

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



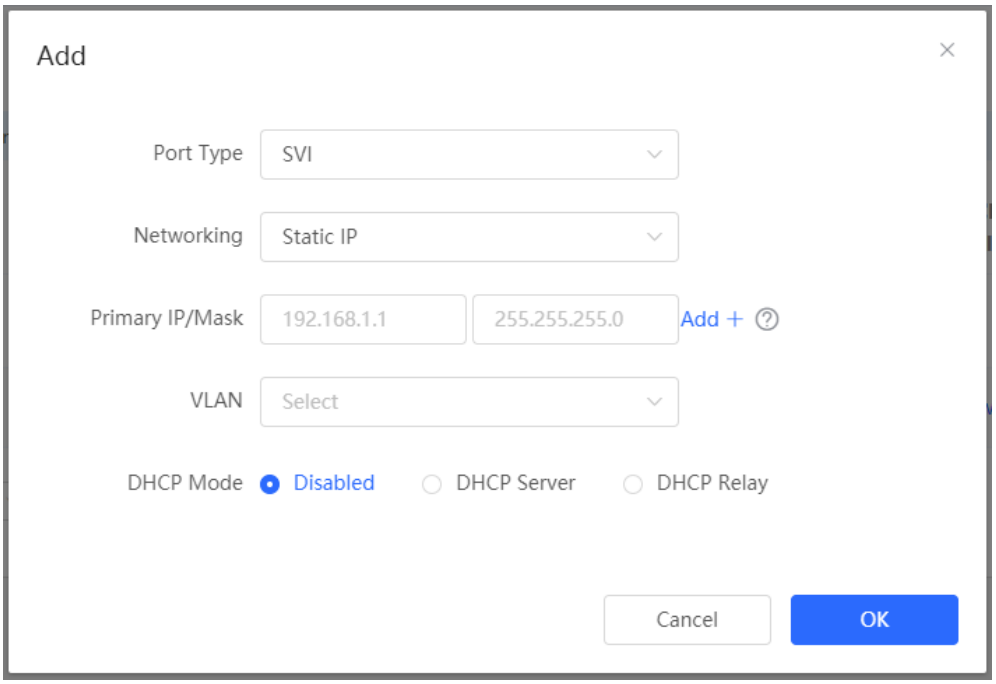


Table 6-1 Description of Configuration Parameters of L3 Interfaces

Parameter	Description
Port Type	The type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port. For details, see Table 4-1
Networking	Specifies DHCP or static mode for a port to obtain the IP address.
VLAN	Specifies the VLAN, to which an SVI belongs.
IP/Mask	When **Networking** is set to **Static IP**, you need to manually enter the IP address and subnet mask.
Select Port	Select the device port to be configured.
Aggregate	Specifies the aggregate port ID, for example, Ag1, when an L3 aggregate port is created.

Parameter	Description
DHCP Mode	Select whether to enable the DHCP service on the L3 interface. **Disabled**: Indicates that the DHCP service is disabled. No IP address can be assigned to clients connected to the interface. **DHCP Server**: Indicates that the device functions as the DHCP server to assign IP addresses to downlink devices connected to the interface. You need to set the start IP address of an address pool, number of IP addresses that can be assigned, and address lease; for more information, see 6.2. **DHCP Relay**: Indicates that the device serves as a DHCP relay, obtains IP addresses from an external server, and assigns the IP addresses to downlink devices. The interface IP address and DHCP server IP address need to be configured. The interface IP address must be in the same network segment as the address pool of the DHCP server.
Excluded IP Address (Range)	When the device acts as a DHCP server, set the IP address in the address pool that is not used for assignment

Note

- VLAN 1 is the default SVI of the device. It can be neither modified nor deleted.
- The management VLAN is only displayed on the **L3 Interfaces** page but cannot be modified. To modify it, choose **Ports** > **MGMT IP**. For details, see 4.6 .
- The DHCP relay and DHCP server functions of an L3 interface are mutually exclusive and cannot be configured at the same time.
- Member ports of an L3 interface must be routed ports.

6.2 Configuring the IPv6 Address for the L3 Interface

IPv6 is a suite of standard protocols for the network layer of the Internet. IPv6 solves the following problems of IPv4:

- Address depletion:

  NAT must be enabled on the gateway to convert multiple private network addresses into a public network address. This results in an extra delay caused by address translation, and may interrupt the connection between devices inside and outside the gateway. In addition, you need to add a mapping to enable access to the intranet devices from the Internet.

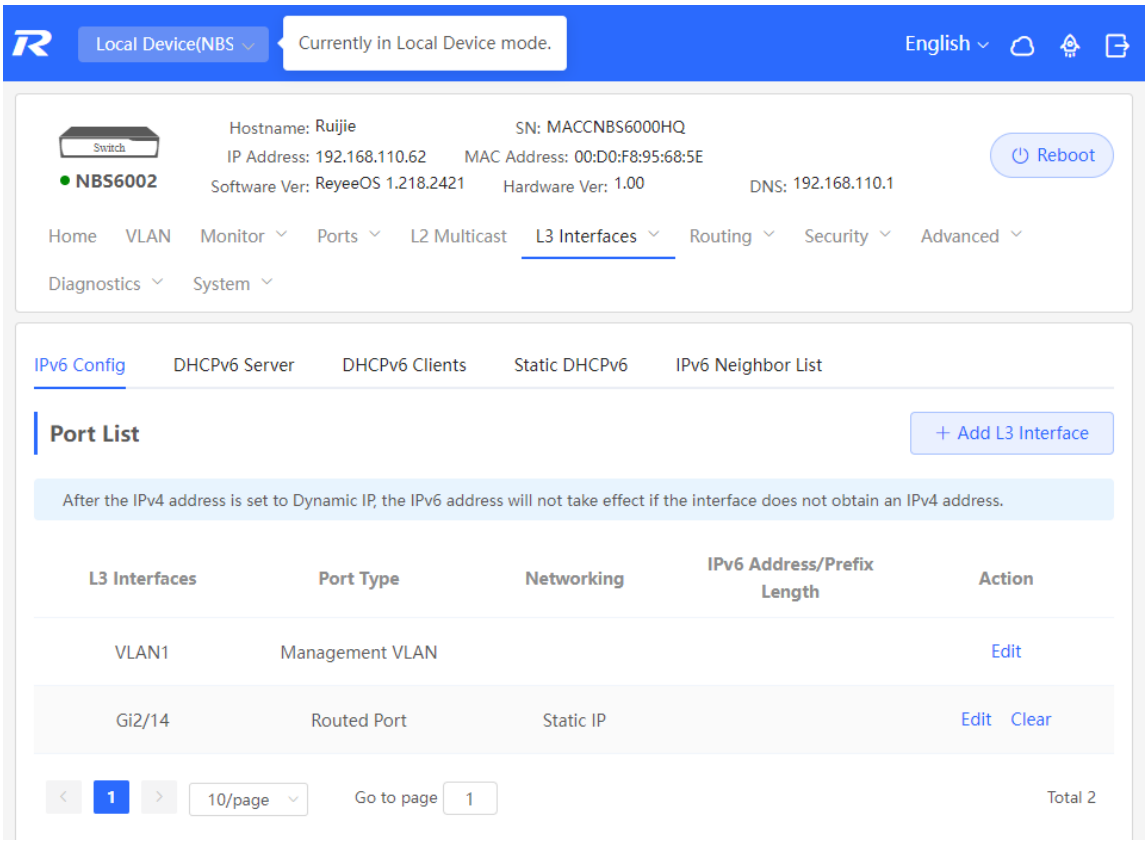
- Design defect:

  IP addresses cannot be formed using network topology mapping, and a large-scale routing table is needed.

- Lack of built-in authentication and confidentiality:

IPv4 itself does not require encryption. It is difficult to trace the source after address translation. As the number of addresses in a network segment is limited, it is easy for attackers to scan all hosts in the LAN. IPv6 integrates IPSec by default. End-to-end connections can be established without address translation, and it is easy to trace the source. IPv6 has a huge address space. A 64-bit prefix address supports 64 host bits, which increases the difficulty and cost of scanning and therefore prevents attacks.

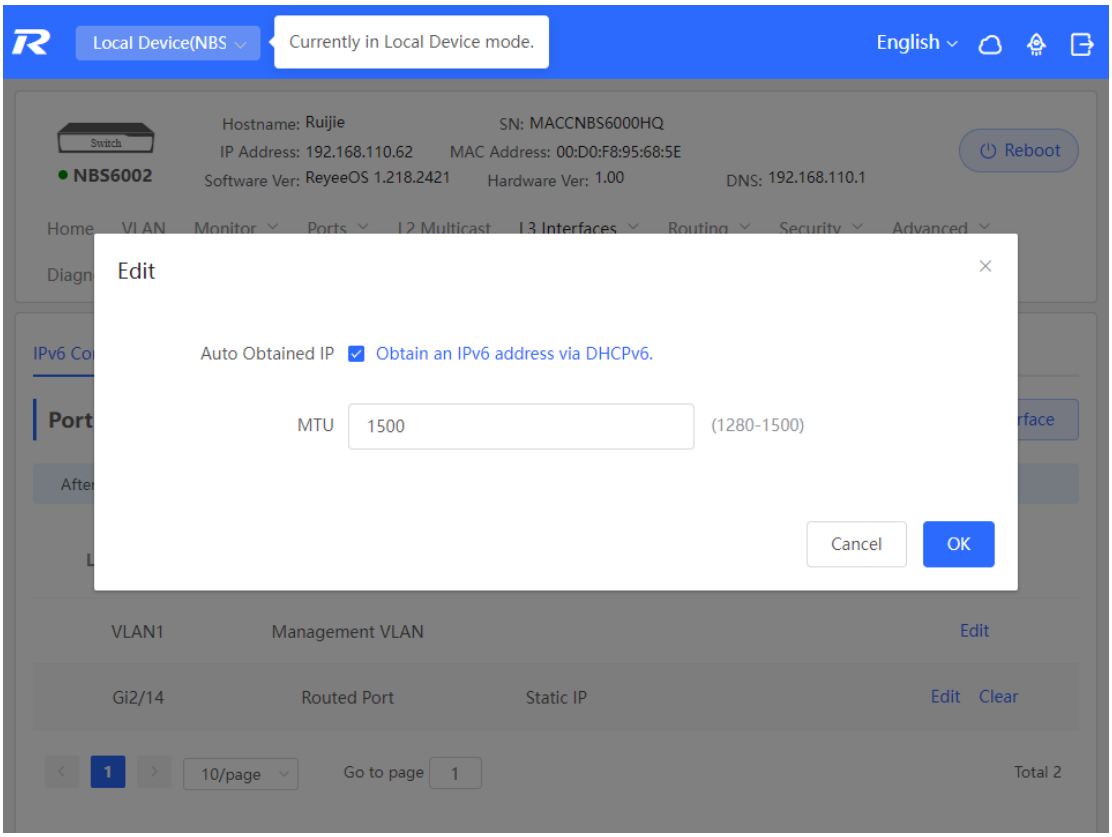
Choose **Local Device** > **L3 Interfaces** > **IPv6 Config**.



Caution

- Add an IPv4 L3 interface first. Then, select the interface on the IPv6 L3 interface configuration page, and click **Edit**.
- If the IPv4 address of an interface is set to **DHCP** and no IPv4 address is obtained, the IPv6 address of this interface will not take effect.

- If an upstream DHCPv6 server is available, select **Auto Obtained IP** and specify the MTU. The default MTU is **1500**. You are advised to retain the default value. Then, click **OK**.



- If no upstream DHCPv6 server is available to assign the IP address, configure the IPv6 information as follows:

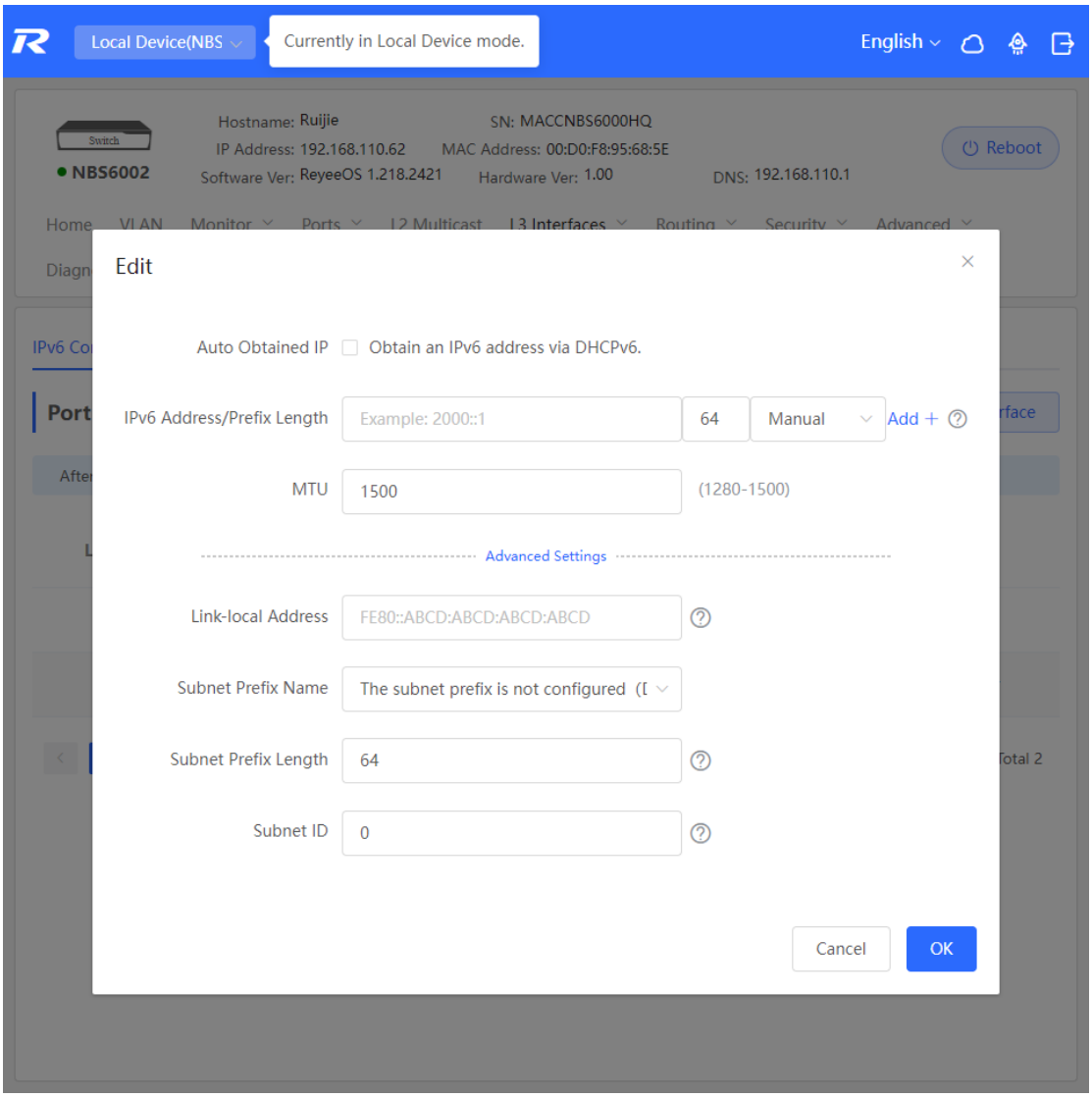


Table 6-2 **IPv6 Address Configuration Parameters of the L3 Interface**

Parameter	Description
Obtain an IPv6 address via DHCPv6	If no upstream DHCPv6 server is available, do not select **Auto Obtained IP**. Instead, manually add the IPv6 address.
IPv6 Address/Prefix Length	Configure the IPv6 address and prefix length. You can click **Add** to add multiple IPv6 addresses. If the primary IP address is empty, the configured secondary IP address is invalid. For manual configuration, the prefix length ranges from 1 to 128. For auto configuration, the prefix length ranges from 1 to 64. If the IPv6 prefix length of the L3 interface is between 48 and 64, this address can be assigned.
MTU	Configure the MTU. The default MTU is **1500**.

Parameter	Description
Advanced Settings	Click **Advanced Settings** to configure the link local address, subnet prefix name, subnet prefix length, and subnet ID.
Link-local Address	The link local address is used to number hosts on a single network link. The first 10 bits of link address in binary notation must be '1111111010'.
Subnet Prefix Name	It identifies a specified link (subnet).
Subnet Prefix Length	It indicates the length (in bits) of the subnet prefix in the address. The value ranges from 48 to 64 (The subnet prefix length must be greater than the length of the prefix assigned by the server).
Subnet ID	Configure the subnet ID of the interface in hexadecimal notation. The number of available subnet IDs is (2^N - 1), where **N** is equal to (Subnet prefix length of the interface - Length of the prefix assigned by the server).

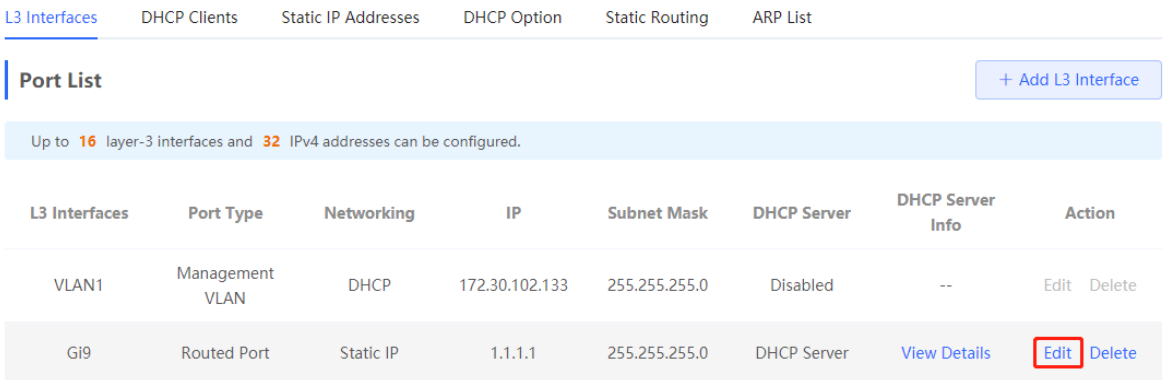
6.3 Configuring the DHCP Service

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

6.3.1 Enable DHCP Services

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

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



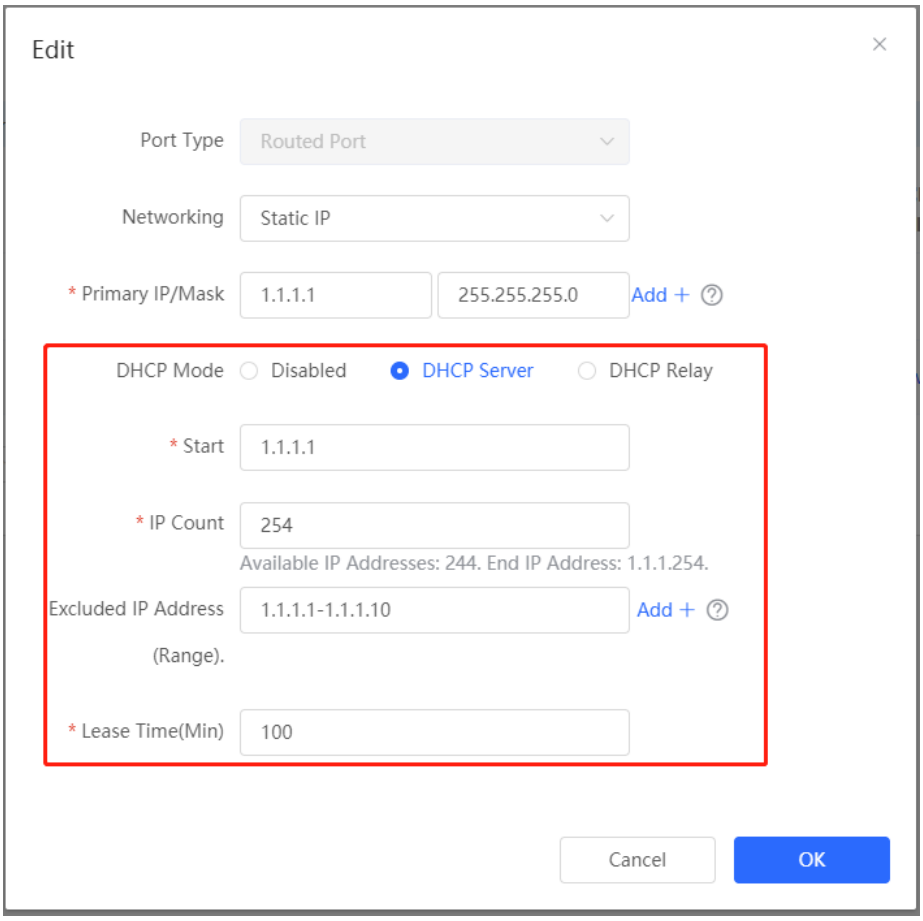


Table 6-3 Description of DHCP Server Configuration Parameters

Parameter	Description
DHCP Mode	To choose DHCP server
Start	The DHCP server assigns the Start IP address automatically, which is the Start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool.
IP Count	The number of IP addresses in the address pool
Excluded IP Address (Range)	IP addresses in the address pool that are not used for allocation, support inputting a single IP address or IP network segment, and add up to 20 address segments.
Lease Time(Min)	The lease of the address, in minutes. **Lease Time(Min)**: When a downlink client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease term expires.

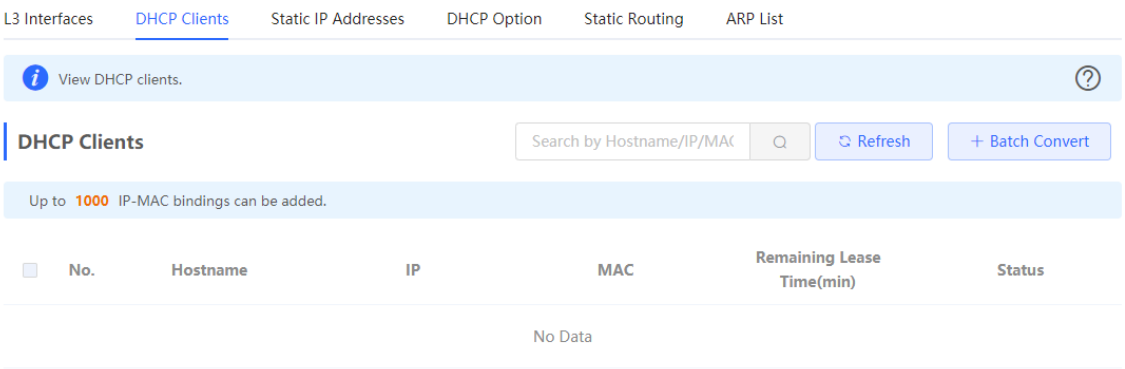
Parameter	Description
	After the downlink client connection is restored, the client can request an IP address again

6.3.2 Viewing the DHCP Client

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

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

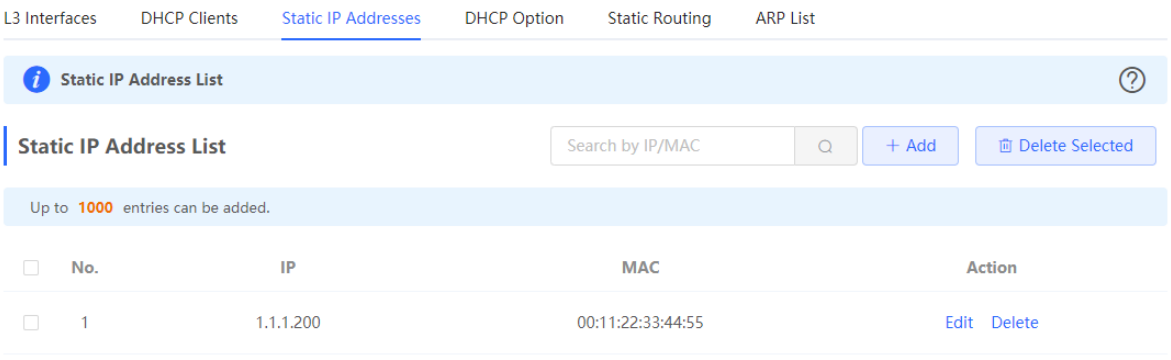
Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Convert**. The dynamic address allocation relationship is added to the static address allocation list, so that the host can obtain the bound IP address for each connection. For details on how to view the static address allocation list, see 6.3.3 .



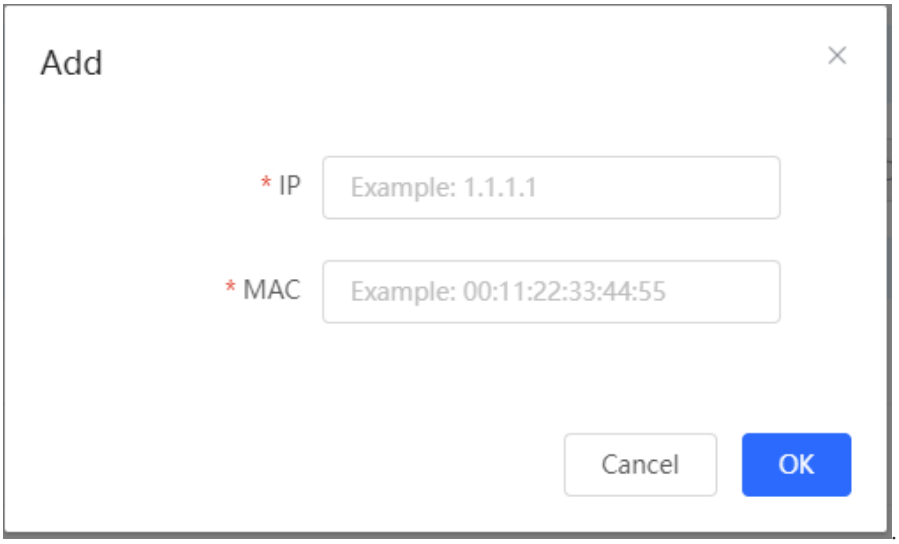
6.3.3 Configuring Static IP Addresses Allocation

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

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



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



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

6.3.4 Configuring the DHCP Server Options

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

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

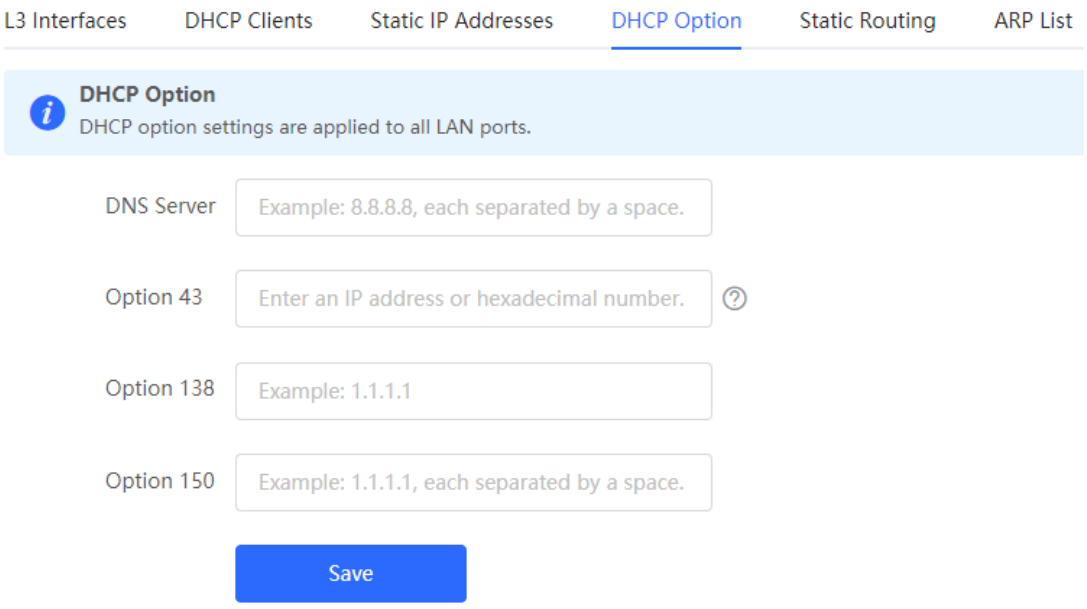


Table 6-4 Description of the DHCP Server Options Configuration Parameters

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

Note

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

6.4 Configuring the DHCPv6 Server

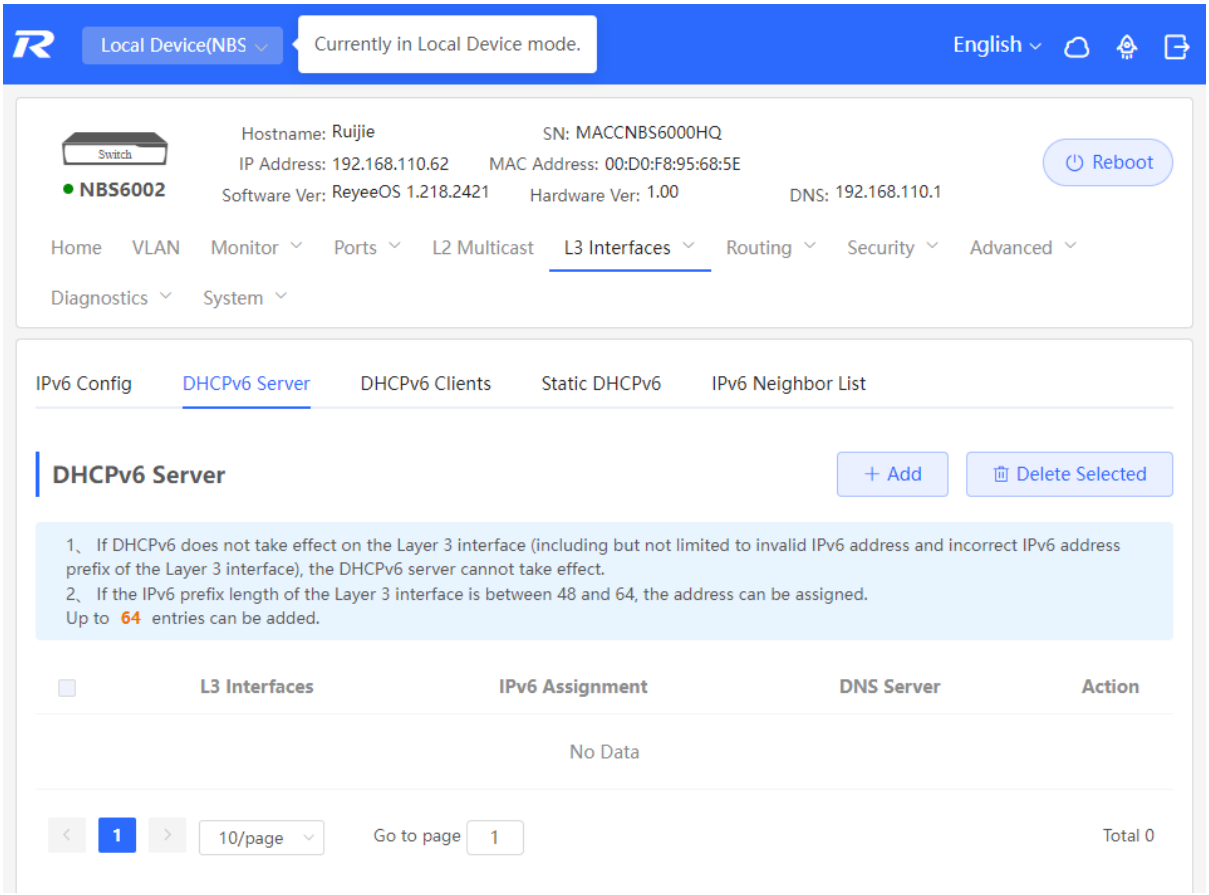
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows the DHCP server to pass configuration information (such as the IPv6 network address) to IPv6 nodes.

Compared with other IPv6 address assignment methods (such as manual configuration and stateless address autoconfiguration), DHCPv6 provides the functions of address assignment, Prefix Delegation (PD), and configuration parameter assignment.

- DHCPv6 is both a stateful address autoconfiguration protocol and a stateless address configuration protocol. It supports flexible addition and reuse of network addresses, and can record the assigned addresses, thus enhancing network management.
- The configuration parameter assignment function of DHCPv6 can solve the problem that parameters cannot be obtained under the stateless address autoconfiguration protocol, and provide the host with configuration information, such as the DNS server address and domain name.

Choose **Local Device** > **L3 Interfaces** > **IPv6 Config**.

(1) Click **Add**, select a L3 interface and IP address assignment method, and enter the address lease term and DNS server address. The address lease term is 30 minutes by default. You are advised to retain the default value. Then, click **OK**.



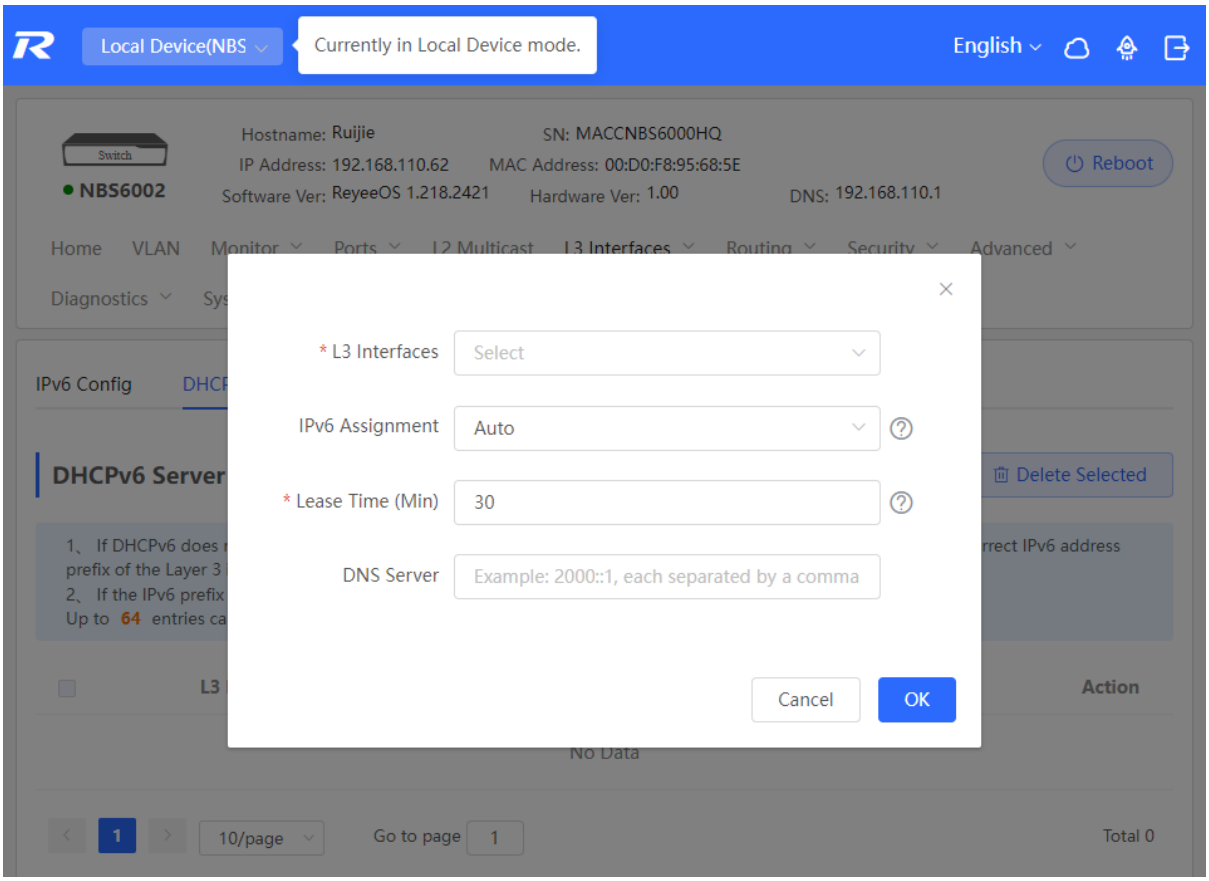


Table 6-5 **IPv6 Address Configuration Parameters of the L3 Interface**

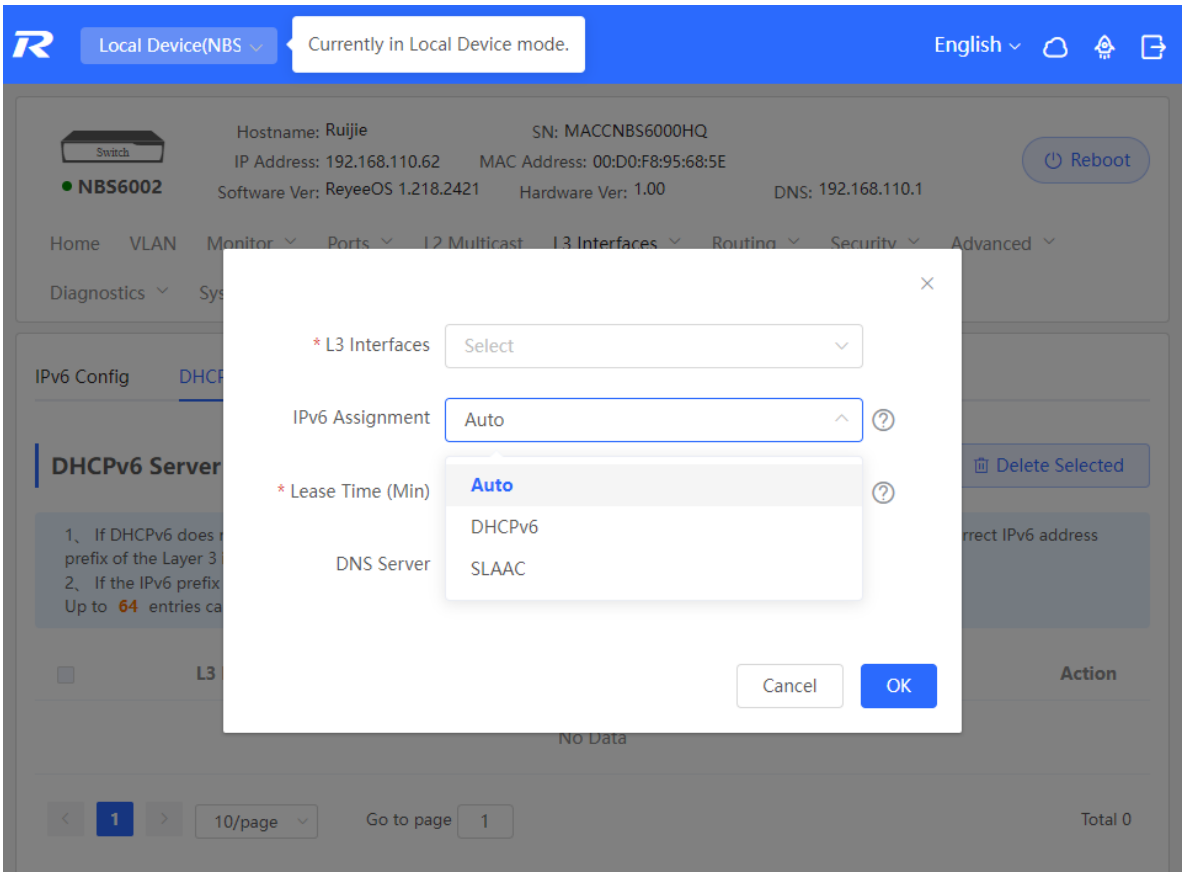
Parameter	Description
L3 Interfaces	Select the L3 interface for which the DHCPv6 server needs to be added.
IPv6 Assignment	If this parameter is set to **Auto**, both DHCPv6 and SLAAC are used to assign IPv6 addresses.
Lease Time	The default value is **30** minutes. The value ranges from 30 to 2880 minutes. When the device stays online and the network is normal, this parameter is periodically updated (reset to 0).
DNS Server	Enter the DNS server address.

6.4.1 Viewing DHCPv6 Clients

View the information of the client that obtains the IPv6 address from the device, including the host name, IPv6 address, remaining lease term, DHCPv6 Unique Identifier (DUID), and status. Click + Batch Convert to bind the IP addresses and hosts in batches, so that the IP addresses obtained by the hosts from the switch remain unchanged.

Note

Each server or client has only one DUID for identification.

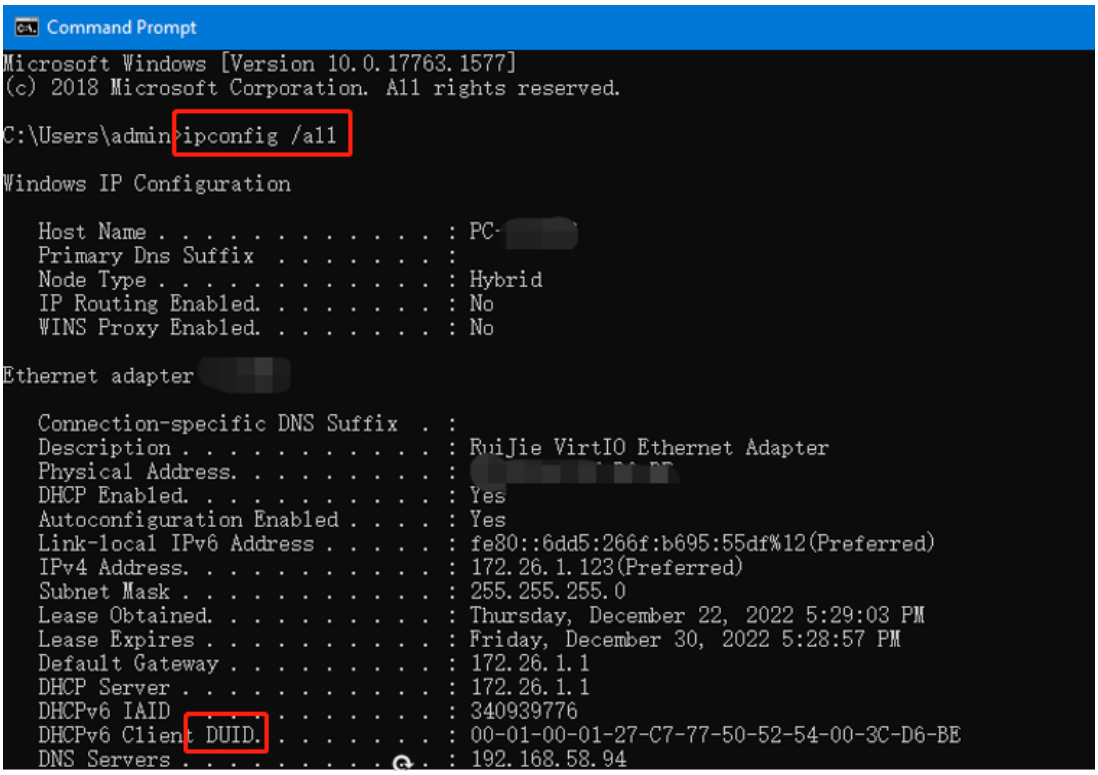


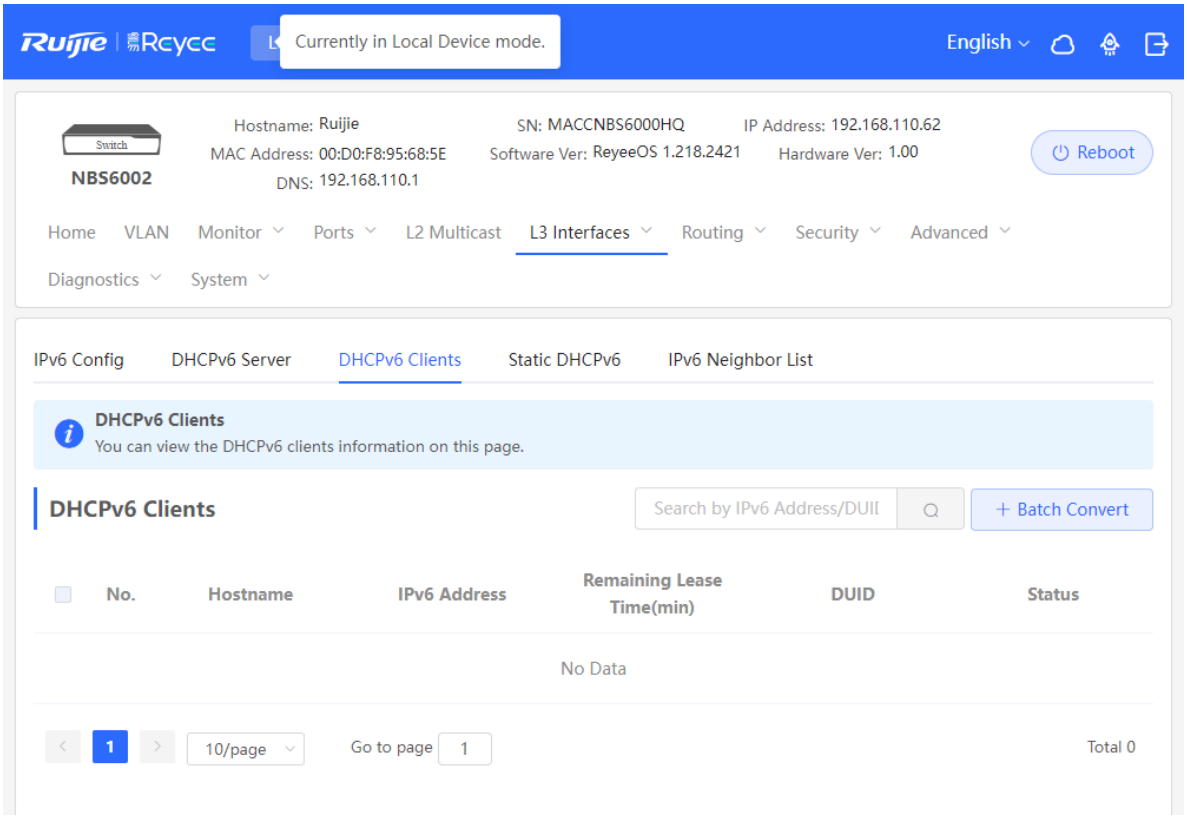
6.4.2 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

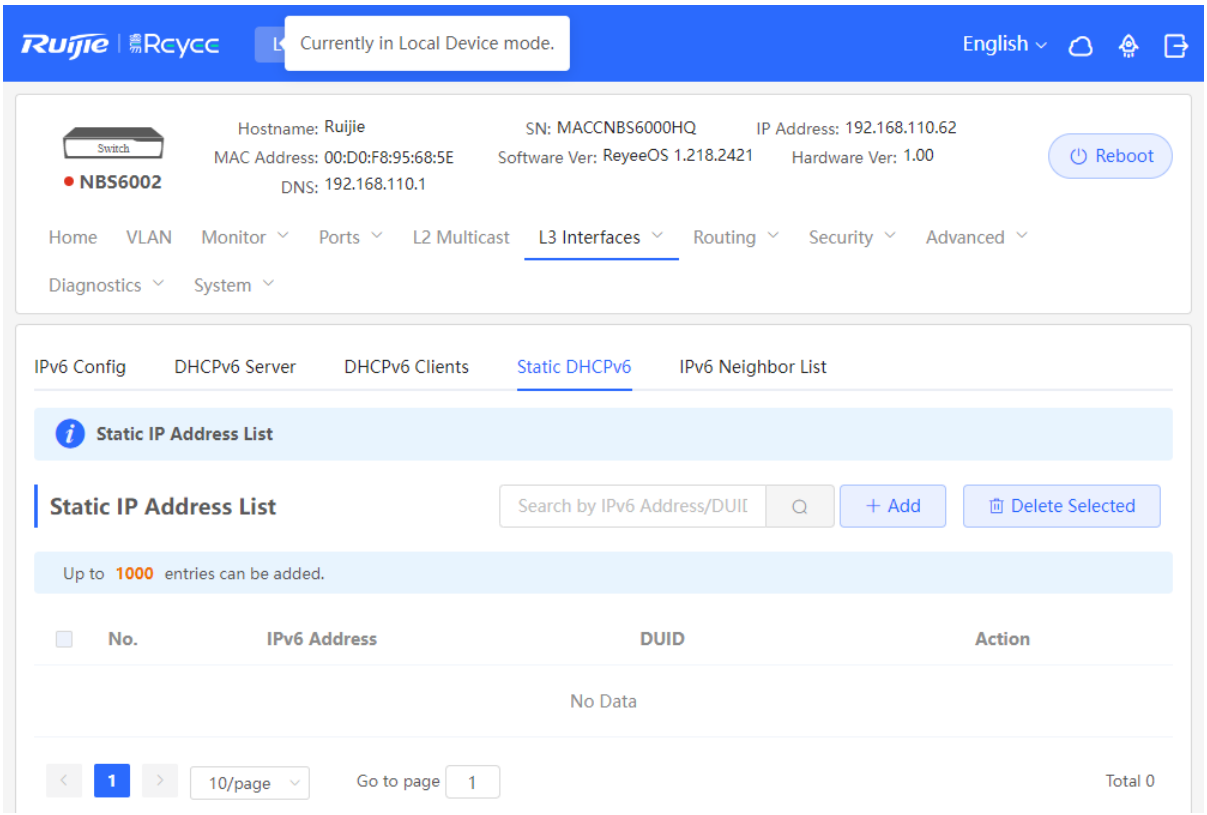
Choose **Local Device** > **L3 Interfaces** > **IPv6 Config** > **Static DHCPv6**.

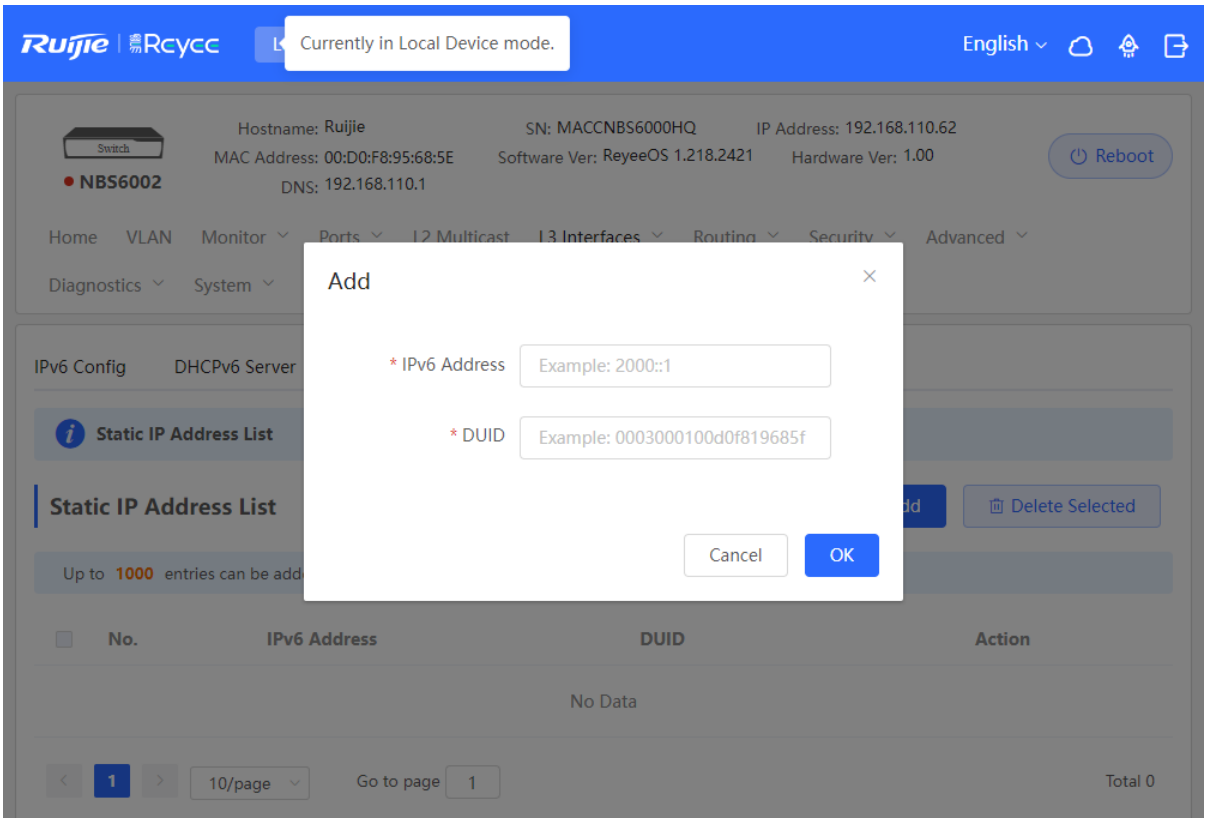
Click **Add**, and enter the IPv6 address and DUID. You are advised to bind the IPv6 address and DUID in the client list. You can run the **ipconfig /all** command on the Command Prompt in Windows to view the DUID.





You can view the DHCPv6 clients information on this page.


Currently in Local Device mode.
English
Hostname: Ruijie
MAC Address: 00:D0:F8:95:68:5E
DNS: 192.168.110.1
SN: MACCNBS6000HQ
Software Ver: ReyeeOS 1.218.2421
IP Address: 192.168.110.62
Hardware Ver: 1.00
NBS6000
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced
Diagnostics System
IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List
Static IP Address List
Static IP Address List
Search by IPv6 Address/DUI
+ Add
Delete Selected
Up to 1000 entries can be added.
No. IPv6 Address DUID Action
No Data
1
10/page
Go to page 1
Total 0


Currently in Local Device mode.
English
Hostname: Ruijie
MAC Address: 00:D0:F8:95:68:5E
DNS: 192.168.110.1
SN: MACCNBS6000HQ
Software Ver: ReyeeOS 1.218.2421
IP Address: 192.168.110.62
Hardware Ver: 1.00
NBS6000
Reboot
Add
* IPv6 Address
Example: 2000::1
* DUID
Example: 0003000100d0f819685f
Cancel
OK
Delete Selected
No. IPv6 Address DUID Action
No Data
10/page
Go to page 1
Total 0

6.5 Configuring the IPv6 Neighbor List

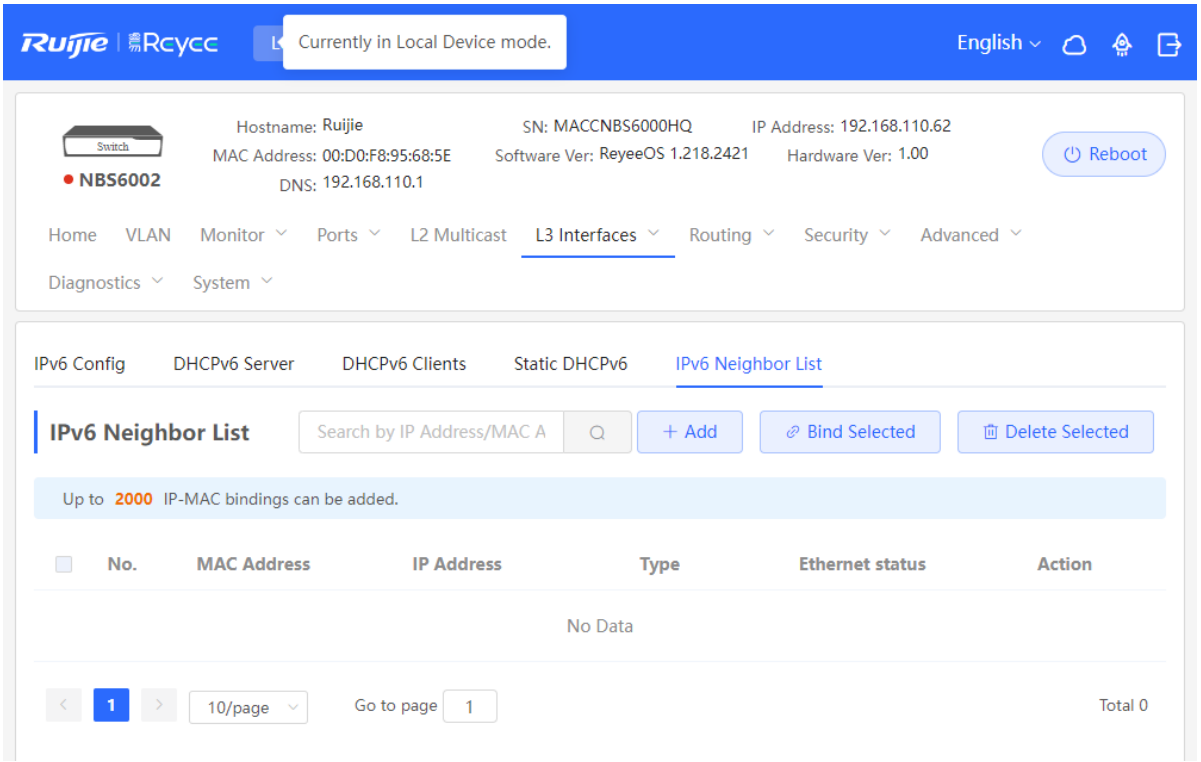
In IPv6, Neighbor Discovery Protocol (NDP) is an important basic protocol. NDP replaces the ARP and ICMP route discovery protocols of IPv4, and supports the following functions: address resolution, neighbor status tracking, duplicate address detection, router discovery, and redirection.

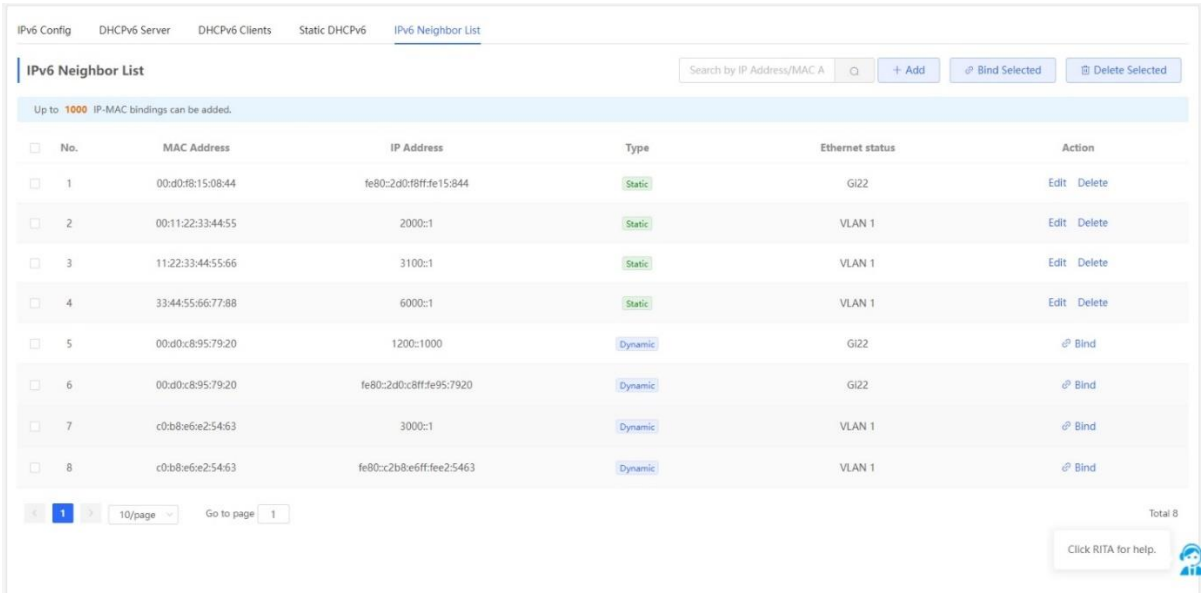
Choose **Local Device** > **L3 Interfaces** > **IPv6 Config** > **IPv6 Neighbor List**.

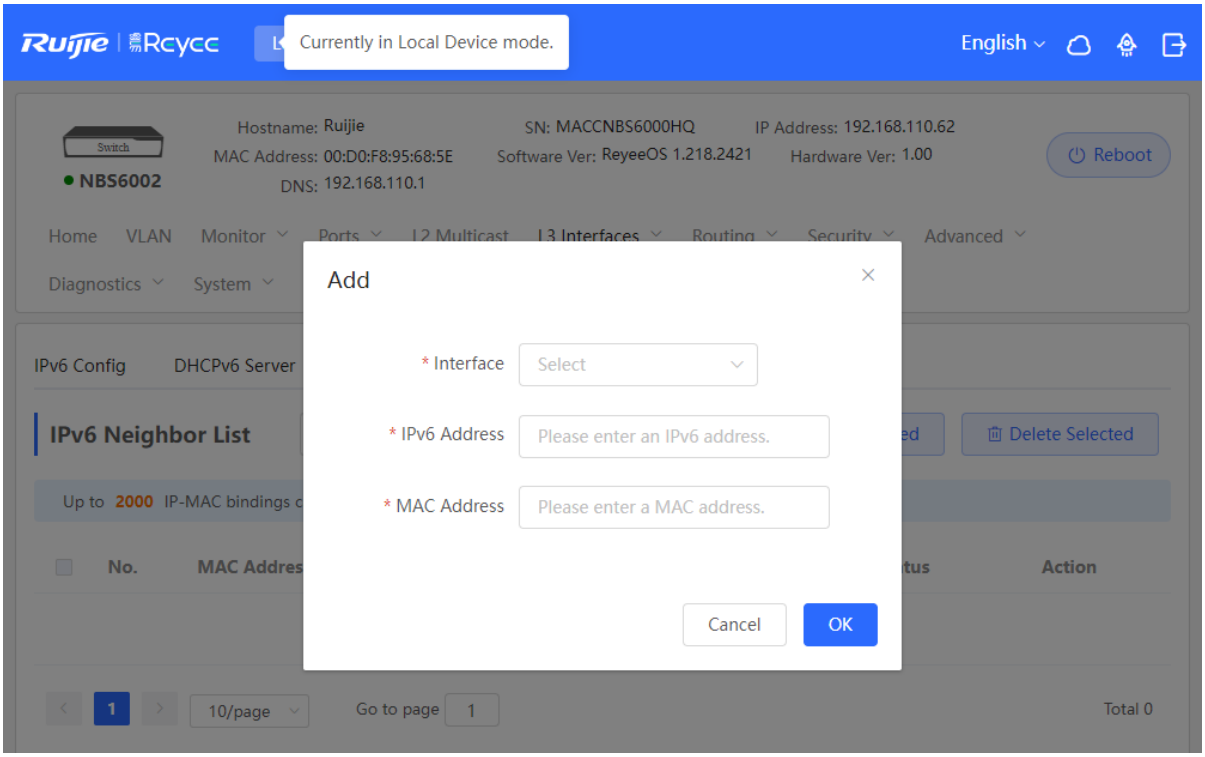
Click **Add** and manually add the interface, IPv6 address and MAC address of the neighbor.

Click **Bind Selected** to bind the IPv6 address and MAC address in the list to prevent ND attacks.

You can also modify, delete, batch delete, or search neighbors (by IP address or MAC address).







6.6 Configuring a Static ARP Entry

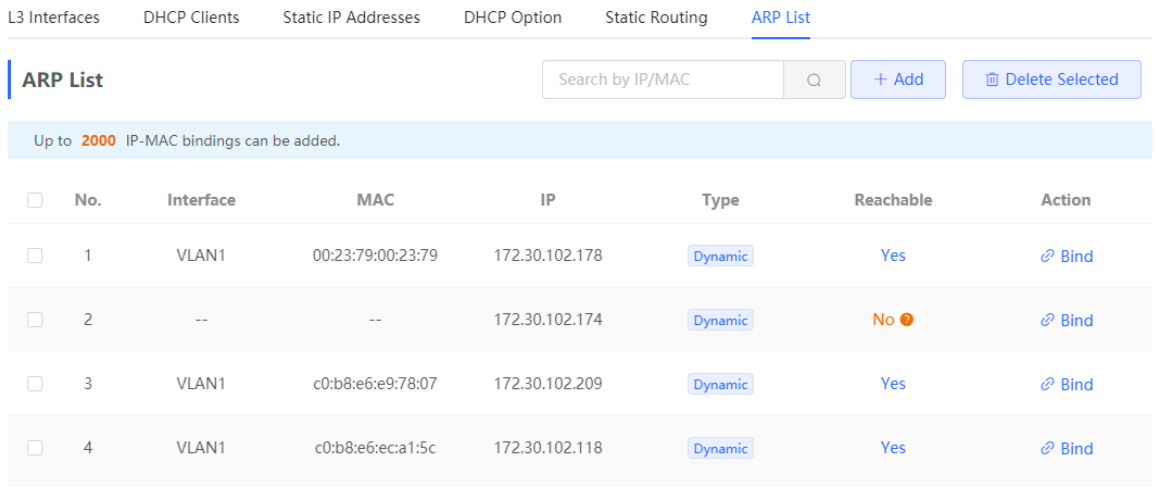
Choose **Local Device** > **L3 Interfaces** > **ARP List**.

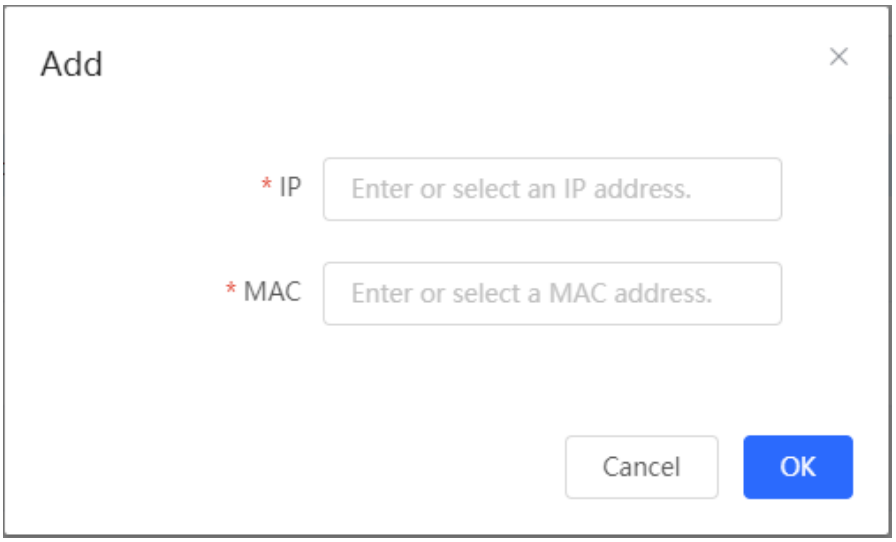
The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. Supports binding ARP mappings or manually specifying the IP address and MAC address mapping to prevent devices from learning wrong ARP entries and improve network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

- To bind a dynamic ARP entry to a static entry: Select the ARP mapping entry dynamically obtained in the **ARP**

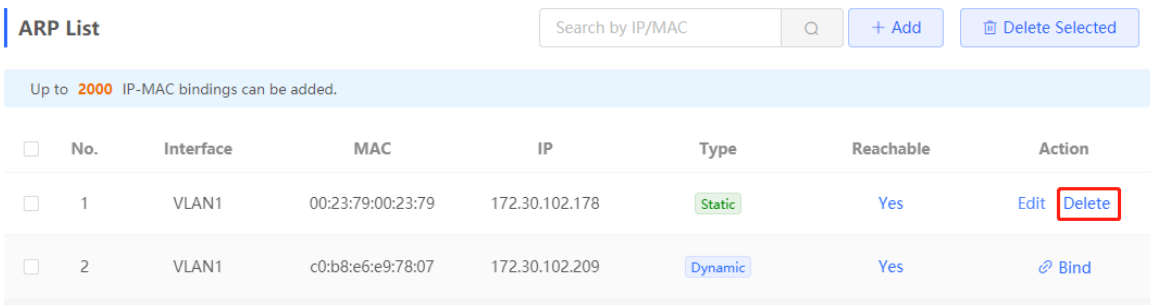
List, and click **Bind** to complete the binding.

- To manually configure a static ARP entry: Click **Add**, enter the IP address and MAC address to be bound, and click **OK**.





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



7 Configuring Route

7.1 Configuring Static Routes

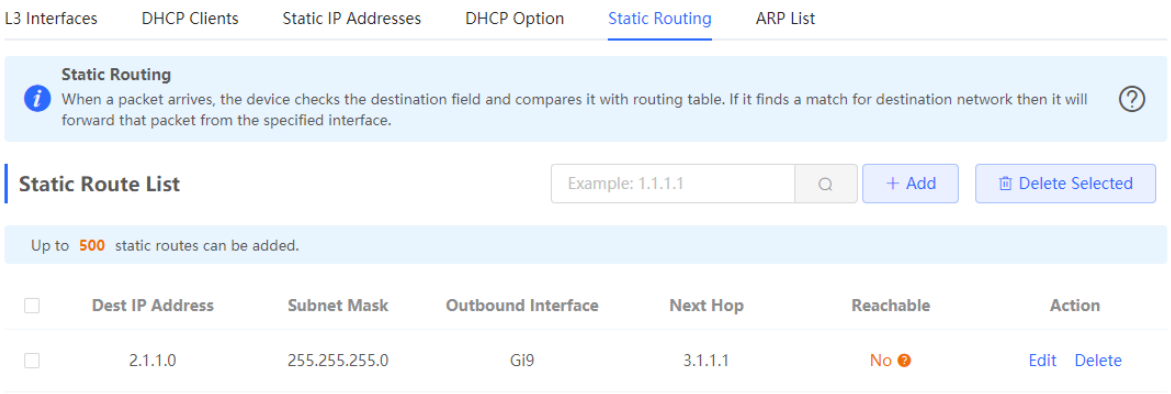
Choose **Local Device** > **L3 Interfaces** > **Static Routing**.

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

Caution

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

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



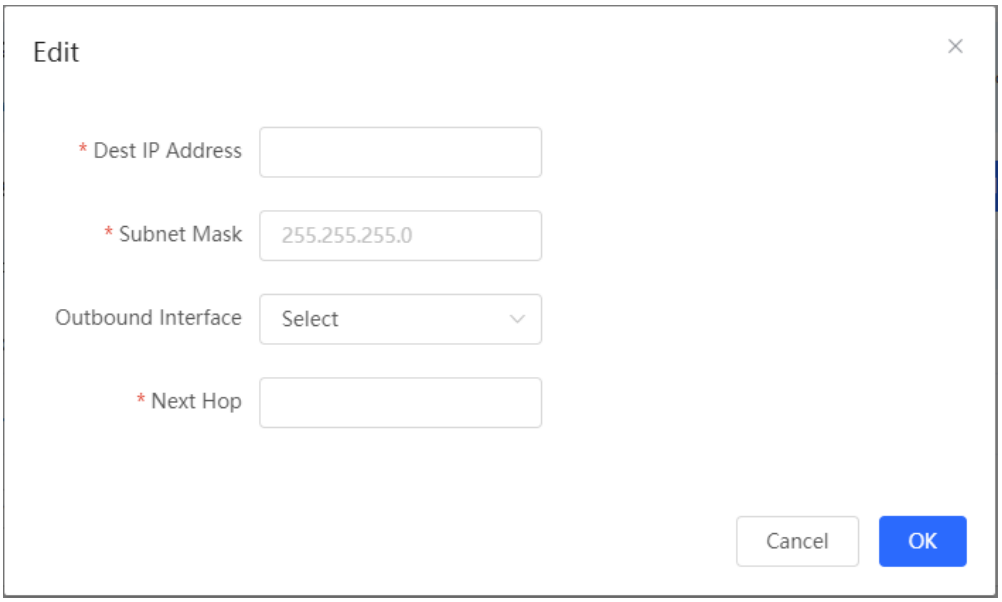
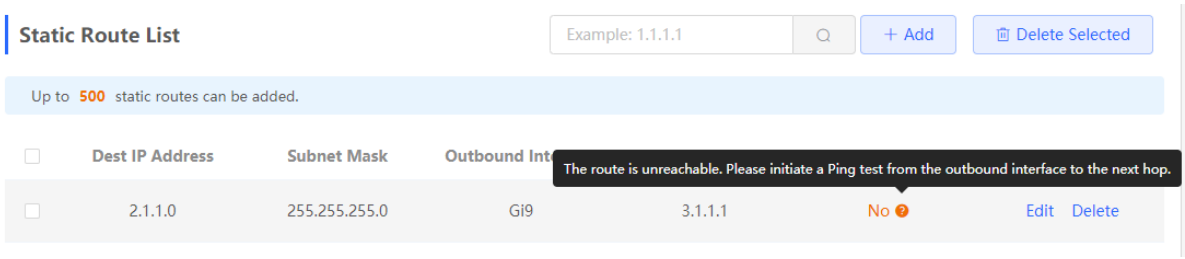


Table 7-1 Description of Static Routes Configuration Parameters

Parameter	Description
Dest IP Address	Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Outbound Interface	Specify the interface that forwards the data packet.
Next Hop	Specify the IP address of the next hop in the route for the data packet

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



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

7.2 Configuring the IPv6 Static Route

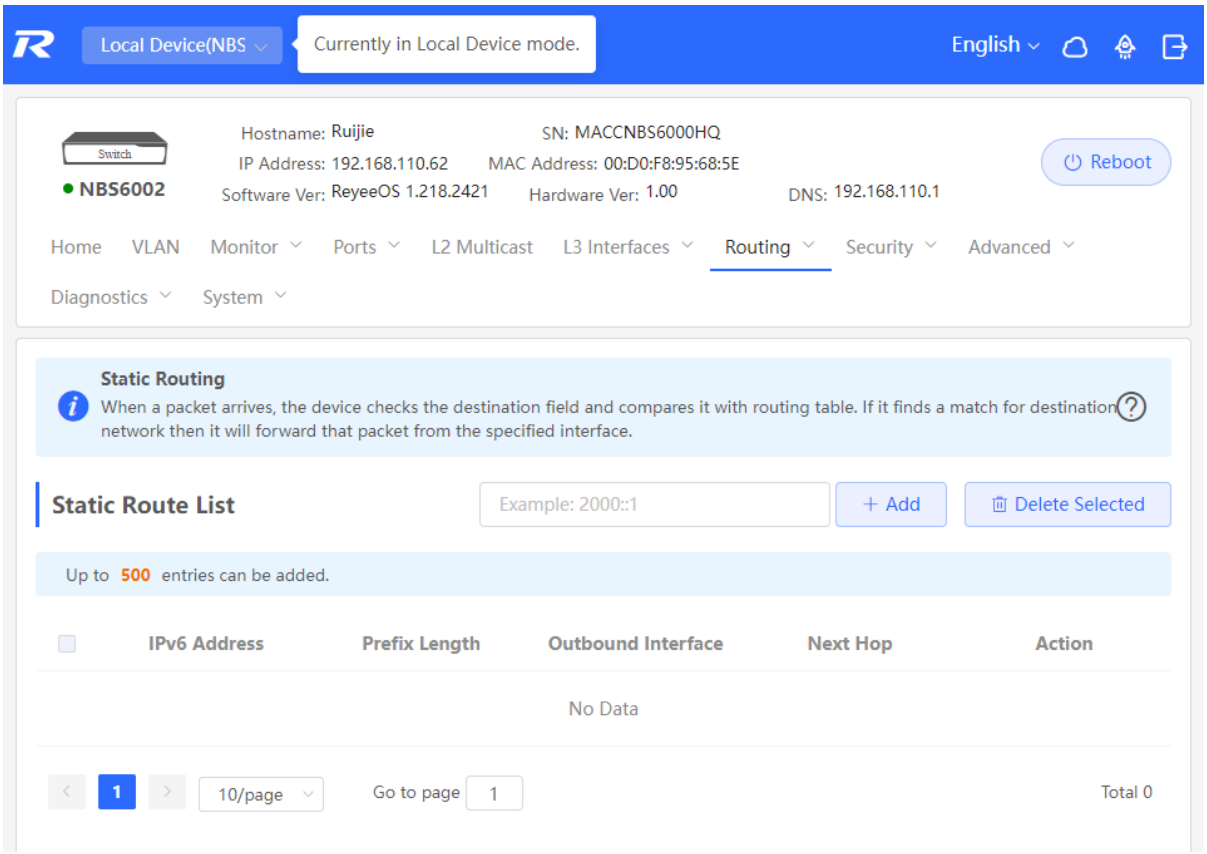
Choose **Local Device** > **Routing** > **Static Routing_v6**.

You need to manually configure an IPv6 static route. When the packet matches the static route, the packet will be forwarded according to the specified forwarding method.

Caution

The static route cannot automatically adapt to changes in the network topology. When the network topology changes, you need to manually reconfigure the static route.

Click **Add**, and enter the destination IPv6 address, length, outbound interface, and next-hop IP address to create a static route.



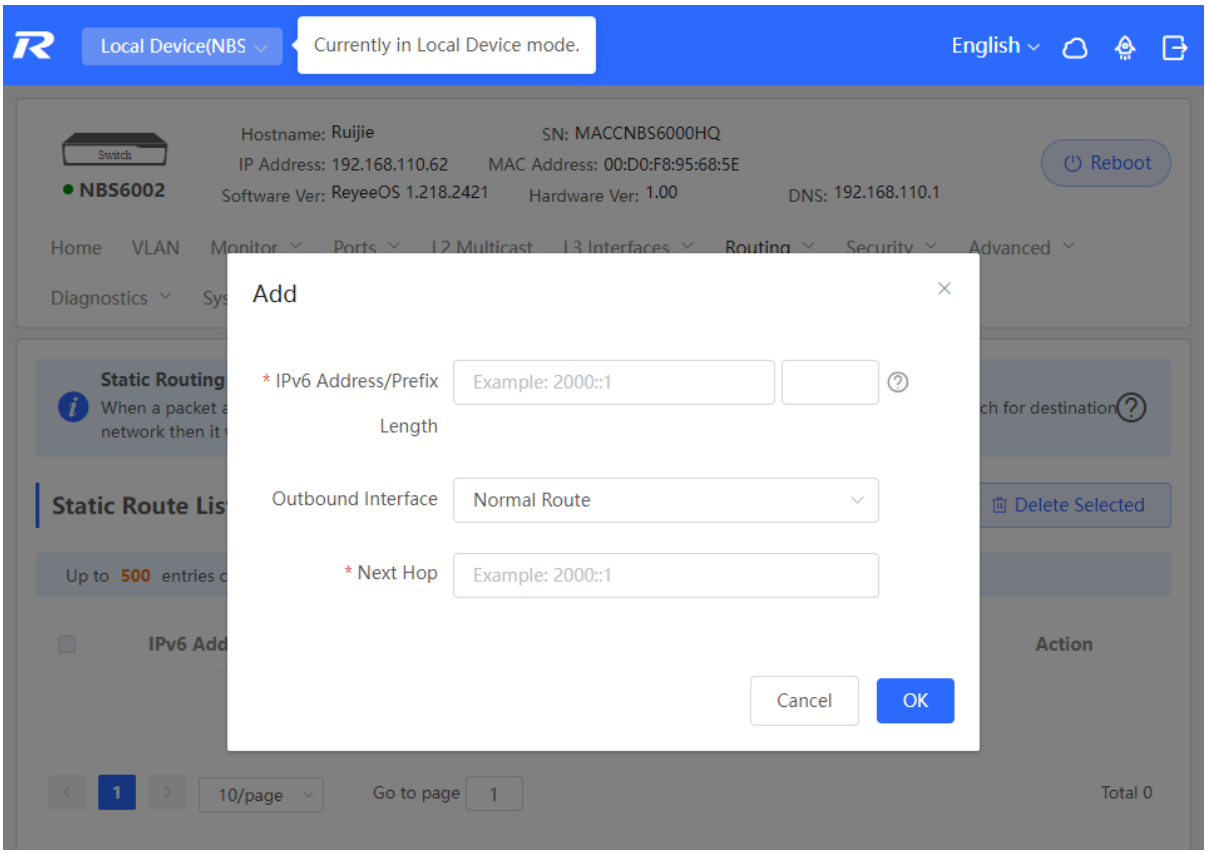


Table 7-2 IPv6 Static Route Configuration Parameters

Parameter	Description
IPv6 Address/Prefix Length	Destination network of the packet. The destination address of the packet is matched according to the IPv6 address and prefix length.
Outbound Interface	Interface that forwards the packet.
Next Hop	IP address of the next routing node to which the packet is sent.

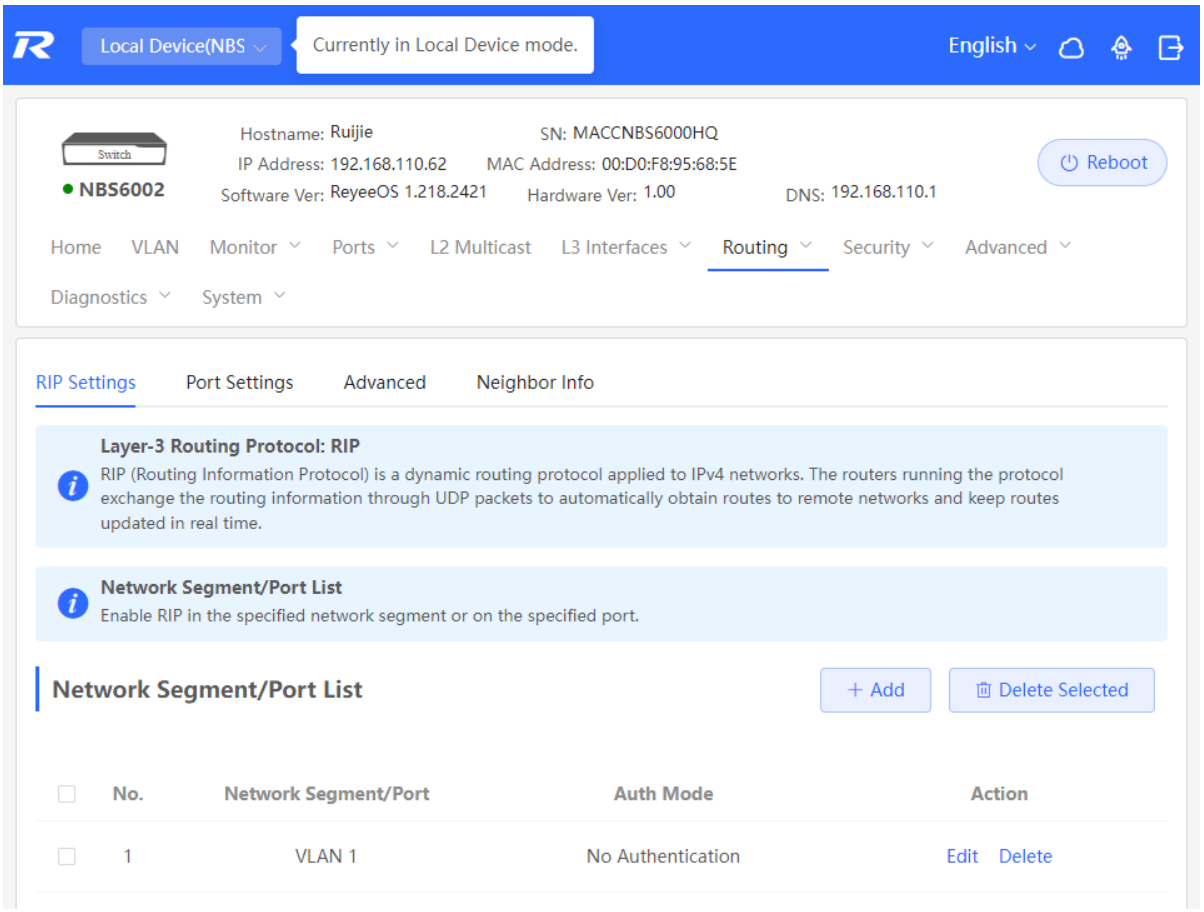
7.3 Configuring RIP

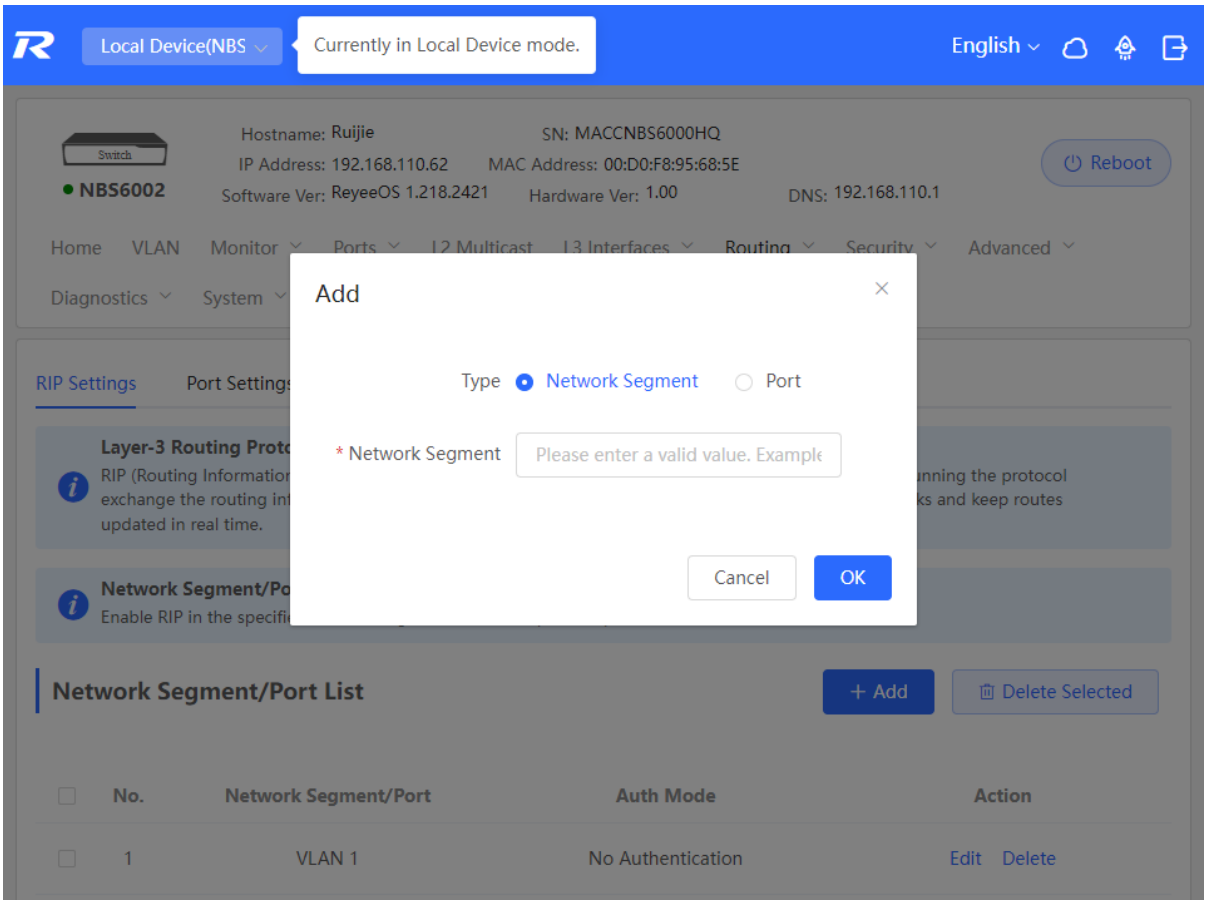
Routing Information Protocol (RIP) is applicable to small and medium-sized networks and is a dynamic routing protocol that is easy to configure. RIP measures the network distance based on the number of hops and selects a route based on the distance. RIP uses UDP port 520 to exchange the routing information.

7.3.1 Configuring RIP Basic Functions

Choose **Local Device** > **Routing** > **RIP Settings**.

Click **Add** and configure the network segment and interface.




Local Device(NBS
Currently in Local Device mode.
English
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
NBS6002
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced
Diagnostics System
RIP Settings
Add
Type Network Segment Port
* Network Segment
Please enter a valid value. Example
Cancel OK
Network Segment/Port List
+ Add
Delete Selected
No. Network Segment/Port Auth Mode Action
1 VLAN 1 No Authentication Edit Delete

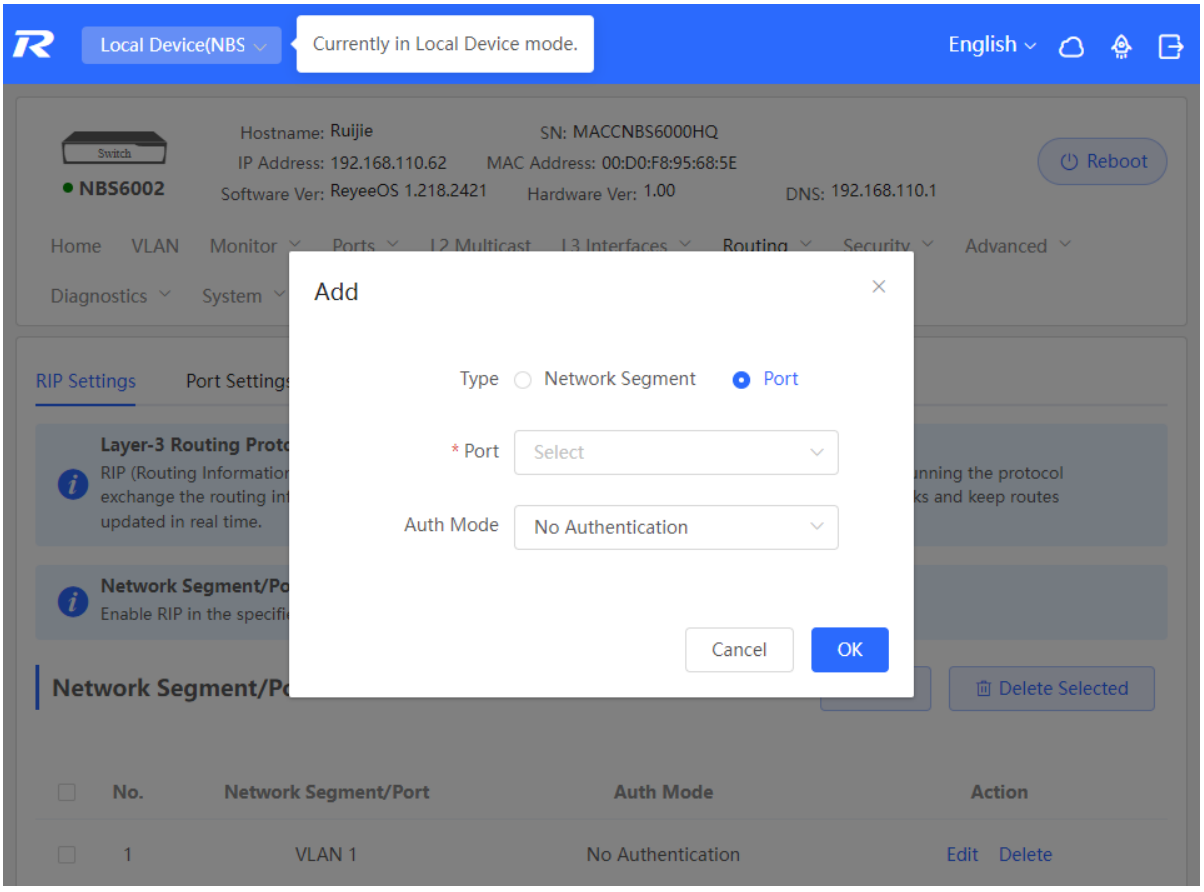

Local Device(NBS
Currently in Local Device mode.
English
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
NBS6002
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced
Diagnostics System
RIP Settings
Add
Type Network Segment Port
* Port
Select
Auth Mode
No Authentication
Cancel OK
Delete Selected
No. Network Segment/Port Auth Mode Action
1 VLAN 1 No Authentication Edit Delete

Table 7-3 RIP Configuration Parameters

Parameter	Description
Type	**Network Segment**: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other. **Port**: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.
Network Segment	Enter the network segment, for example, **10.1.0.0/24**, when **Type** is set to **Network Segment**. RIP will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when **Type** is set to **Port**.
Auth Mode	**No Authentication**: The protocol packets are not authenticated. **Encrypted Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text. **Plain Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when **Auth Mode** is set to **Encrypted Text** or **Plain Text**.

7.3.2 Configuring the RIP Port

Choose **Local Device** > **Routing** > **RIP Settings** > **Port Settings**.

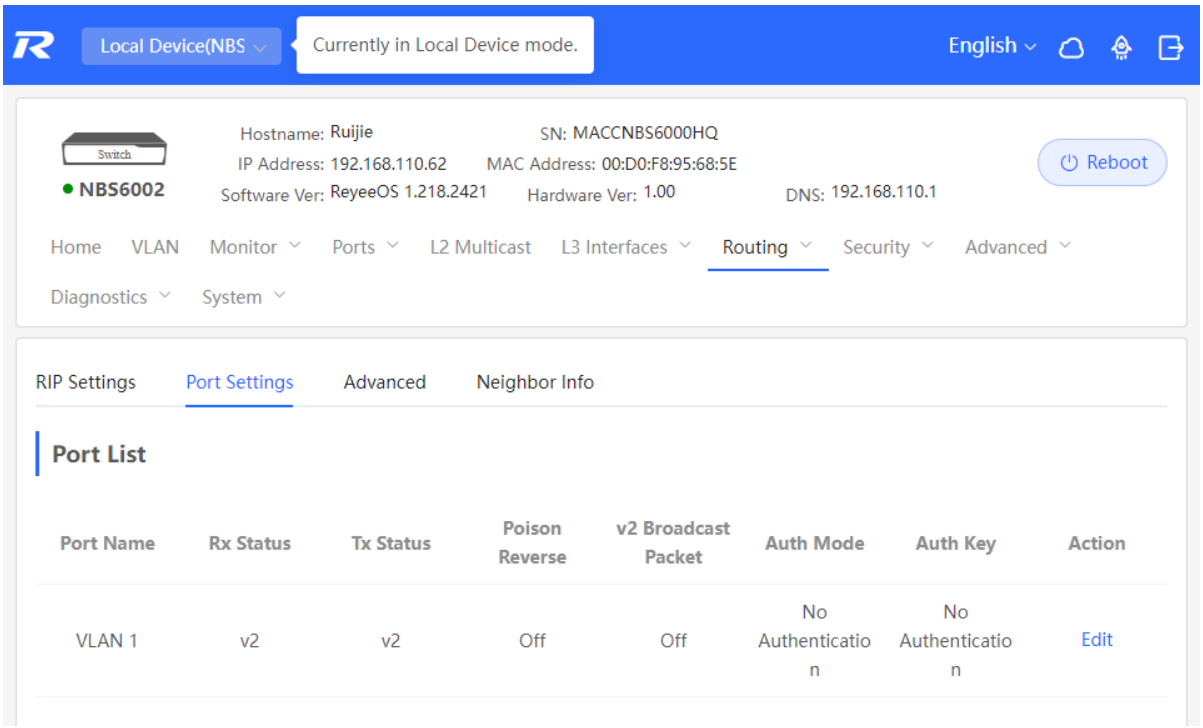


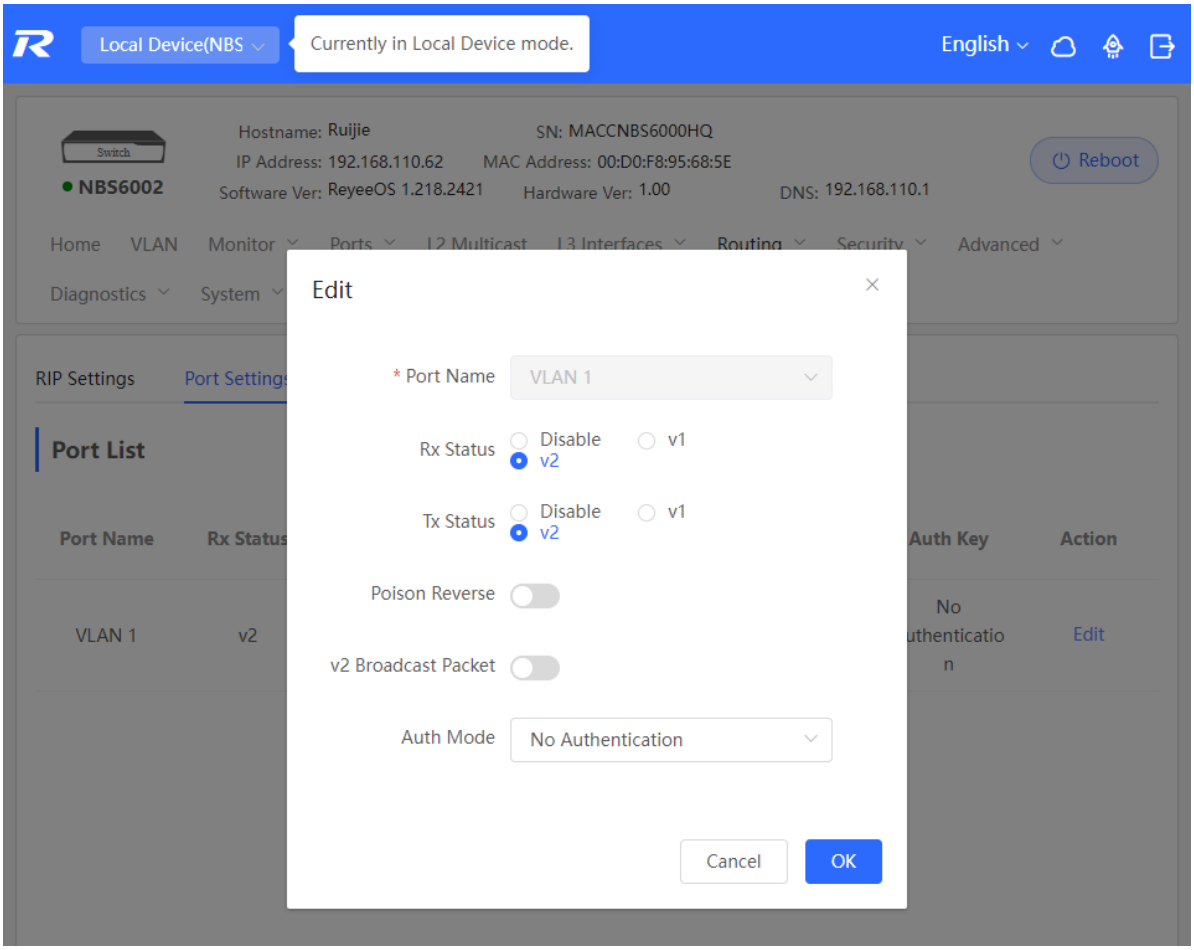
Table 7-4 Configuration Parameters in the Port List

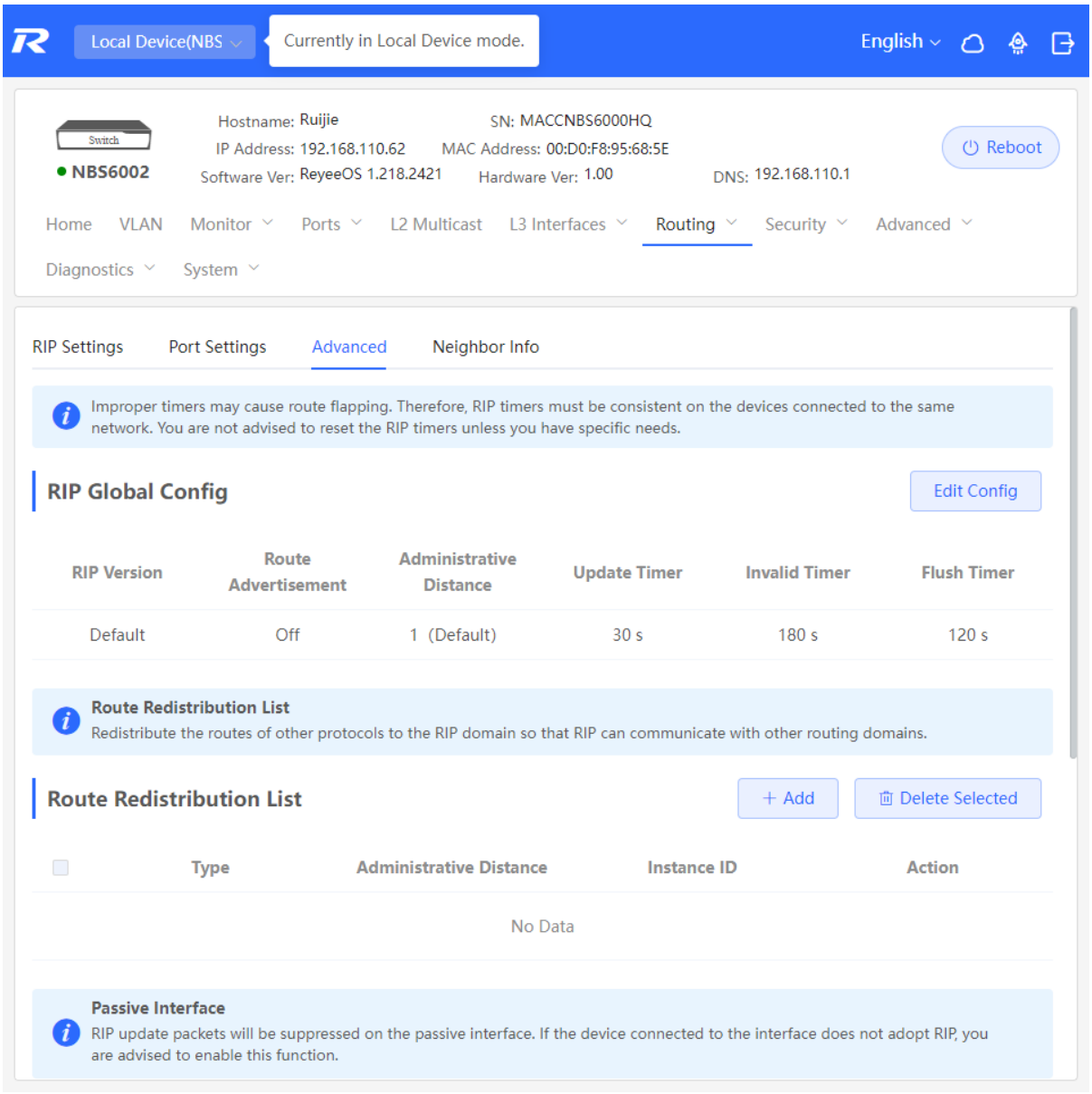
Parameter	Description
Port Name	Name of the port where RIP is enabled.
Rx Status	RIP version of packets currently received.
Tx Status	RIP version of packets currently transmitted.
Poison Reverse	After the port learns the route, the route overhead is set to **16** (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.
v2 Broadcast Packet	When a neighbor does not support multicast, broadcast packets can be sent. You are advised to disable RIPv2 broadcast packets to improve network performance.
Auth Mode	**No Authentication**: The protocol packets are not authenticated. **Encrypted Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of

	encrypted text. **Plain Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when **Auth Mode** is set to **Encrypted Text** or **Plain Text**.
Action	Click **Edit** to modify RIP settings of the port.

7.3.3 Configuring the RIP Global Configuration

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced**, click **Edit**, and configure RIP global configuration parameters.




Local Device(NBS
Currently in Local Device mode.
English
Switch
NBS6002
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
Reboot
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Interfaces
Routing
Security
Advanced
Diagnostics
System
RIP Settings
Port Settings
Advanced
Neighbor Info
Improper timers may cause route flapping. Therefore, RIP timers must be consistent on the devices connected to the same network. You are not advised to reset the RIP timers unless you have specific needs.
RIP Global Config
Edit Config
RIP Version
Route Advertisement
Administrative Distance
Update Timer
Invalid Timer
Flush Timer
Default
Off
1 (Default)
30 s
180 s
120 s
Route Redistribution List
Redistribute the routes of other protocols to the RIP domain so that RIP can communicate with other routing domains.
Route Redistribution List
+ Add
Delete Selected
Type
Administrative Distance
Instance ID
Action
No Data
Passive Interface
RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

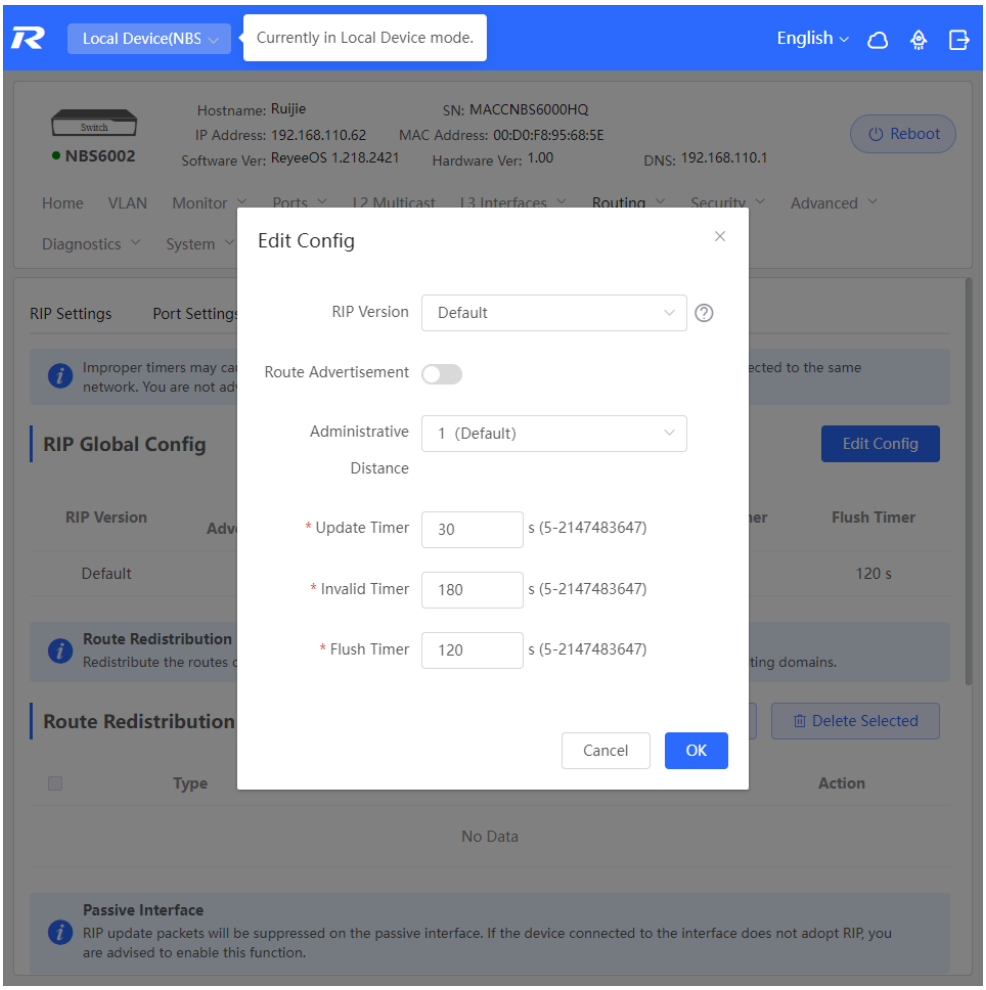


Table 7-5 RIP Global Configuration Parameters

Parameter	Description
RIP Version	**Default**: Select RIPv2 for sending packets and RIPv1/v2 for receiving packets. **V1**: Select RIPv1 for sending and receiving packets. **V2**: Select RIPv2 for sending and receiving packets.
Route Advertisement	After route advertisement is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.

Parameter	Description
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

7.3.4 Configuring the RIP Route Redistribution List

Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced**, click **Add**, and select the type and administrative distance.

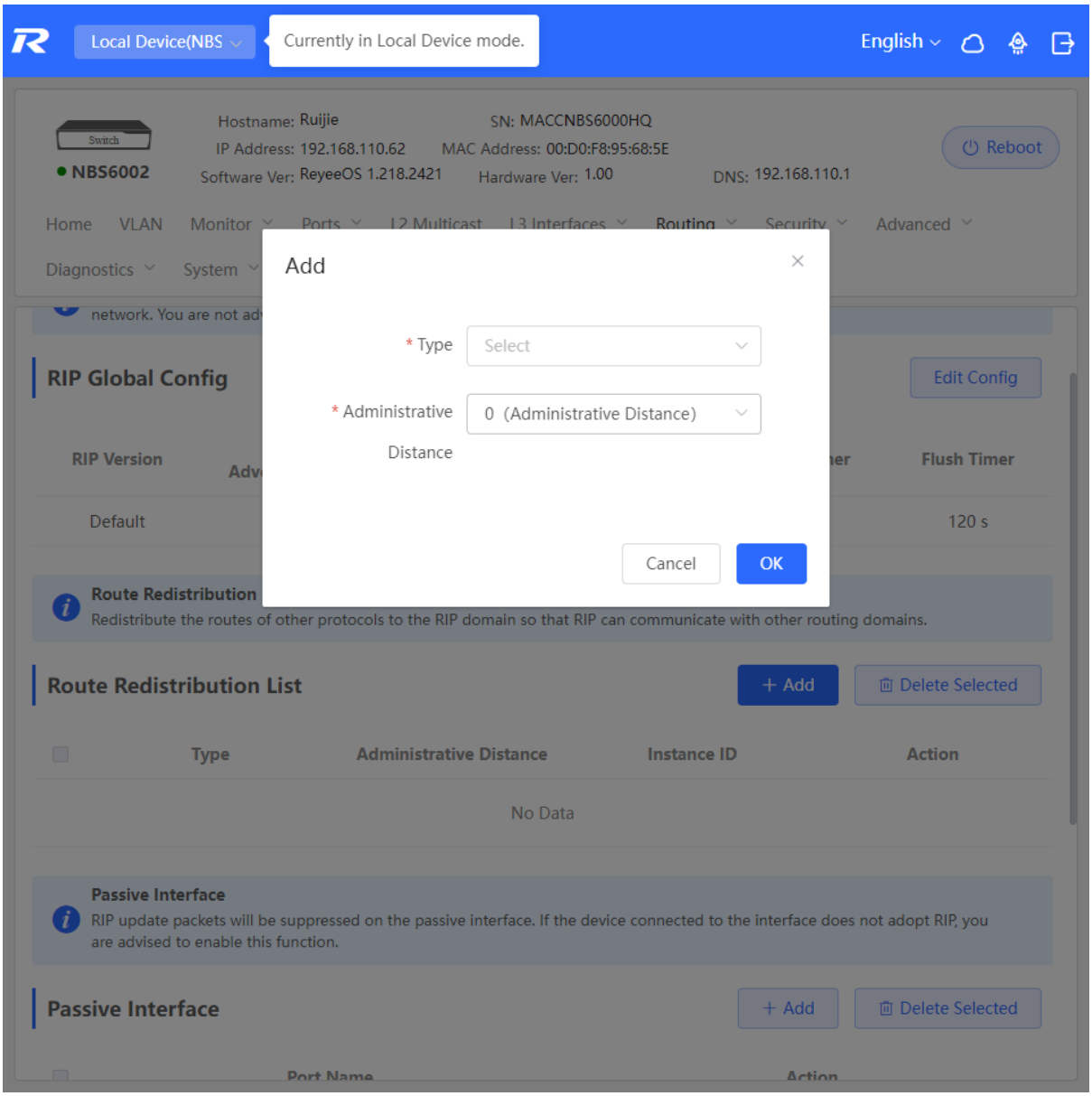
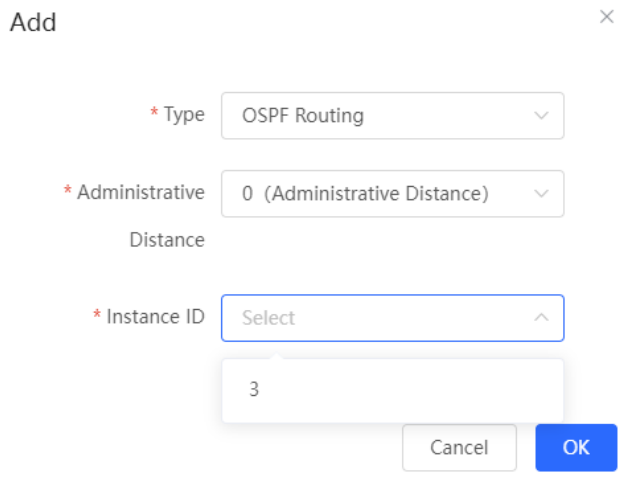


Table 7-6 RIP Route Redistribution Parameters

Parameter	Description
Type	Direct Routing OSPF Routing Static Routing
Administrative Distance	A smaller administrative distance indicates a higher priority. The default value is **0**. The value ranges from 0 to 16.
Instance ID	Select the instance ID of OSPF that needs to be

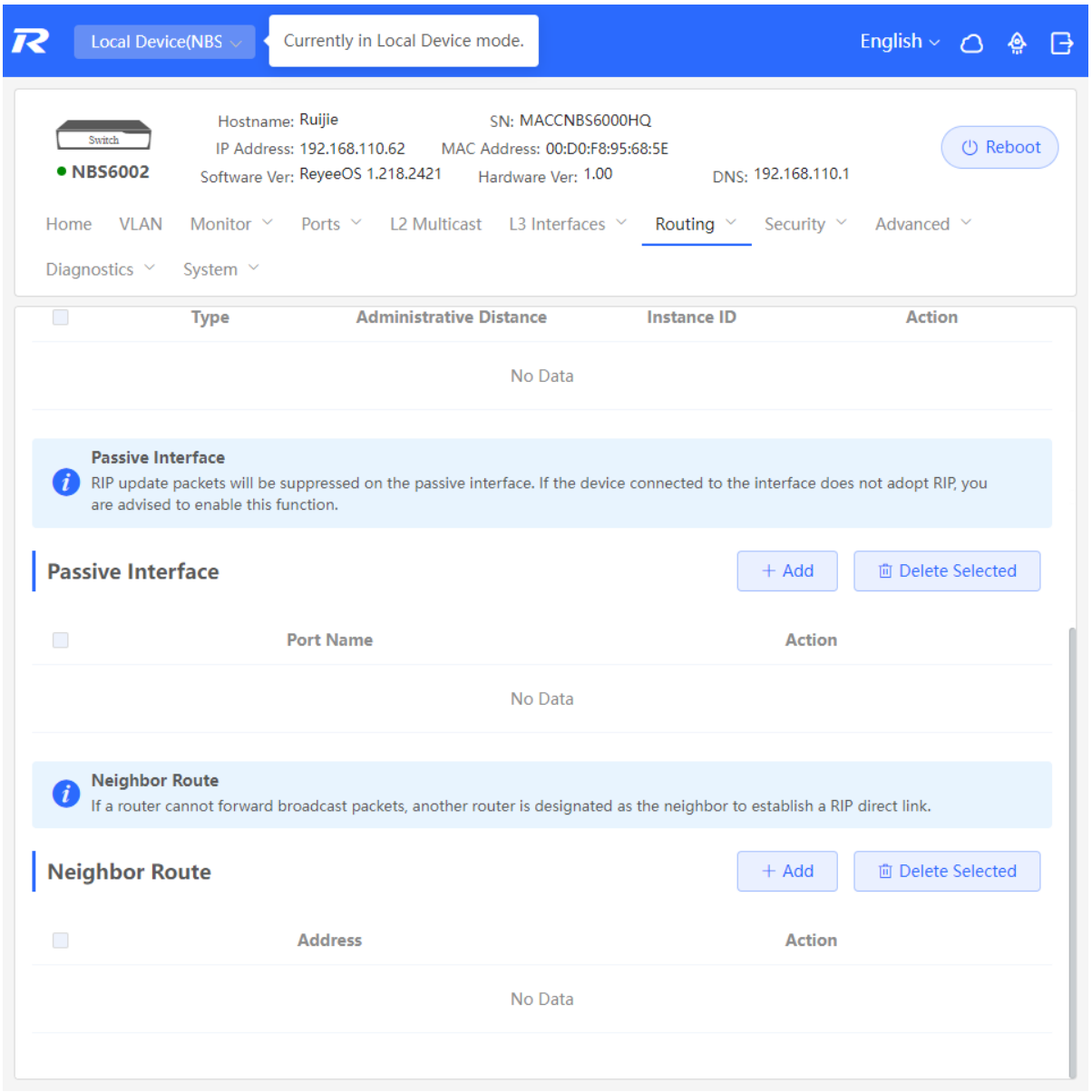
Parameter	Description
	redistributed. OSPFv2 needs to be enabled on the local device.

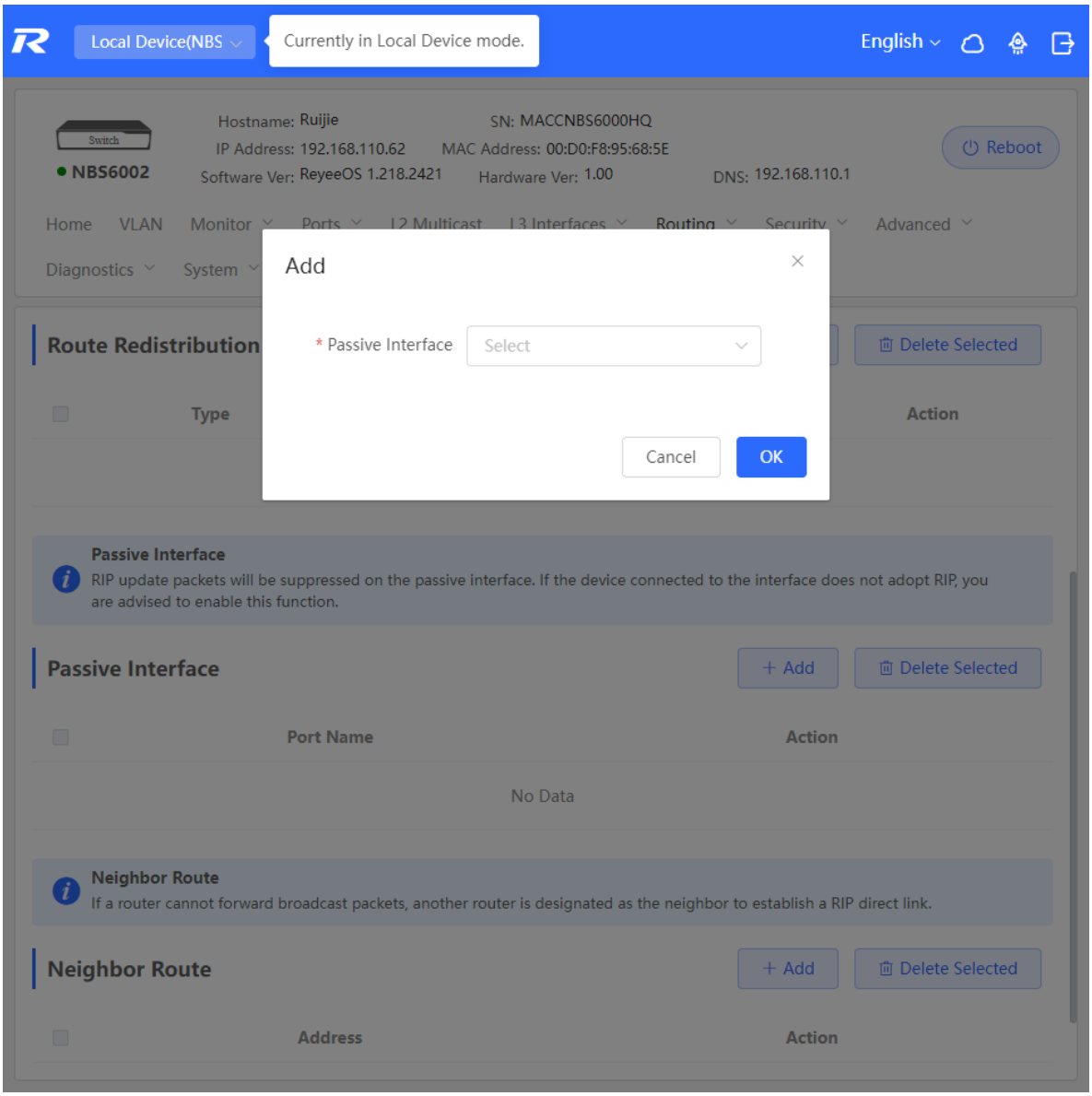


7.3.5 Configuring the Passive Interface

If an interface is configured as a passive interface, it will suppress RIP update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced**, click **Add**, and select a passive interface.

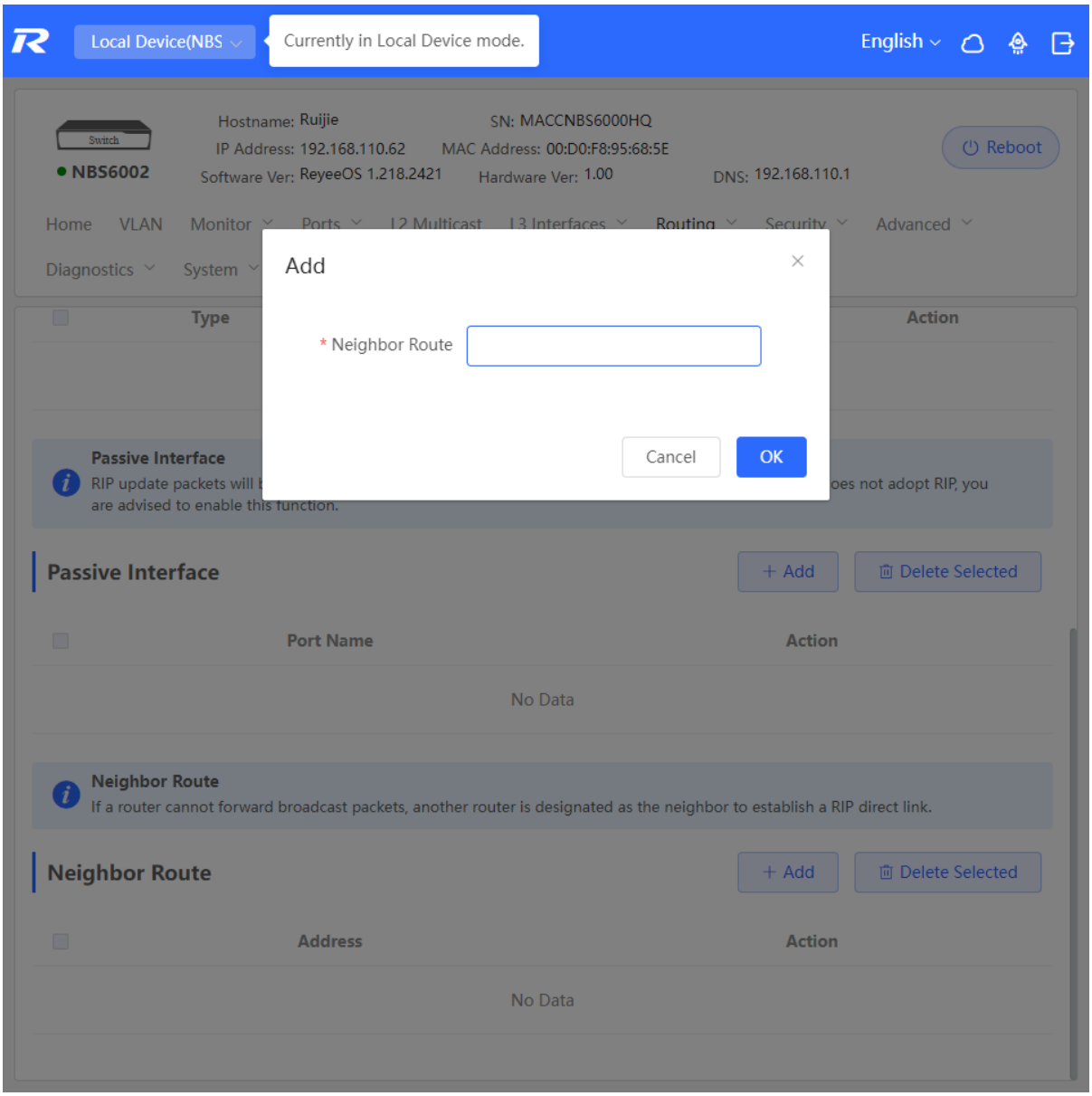

Local Device(NBS
Currently in Local Device mode.
English
Switch
NBS6002
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
Reboot
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Interfaces
Routing
Security
Advanced
Diagnostics
System
Type
Administrative Distance
Instance ID
Action
No Data
Passive Interface
RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.
Passive Interface
+ Add
Delete Selected
Port Name
Action
No Data
Neighbor Route
If a router cannot forward broadcast packets, another router is designated as the neighbor to establish a RIP direct link.
Neighbor Route
+ Add
Delete Selected
Address
Action
No Data

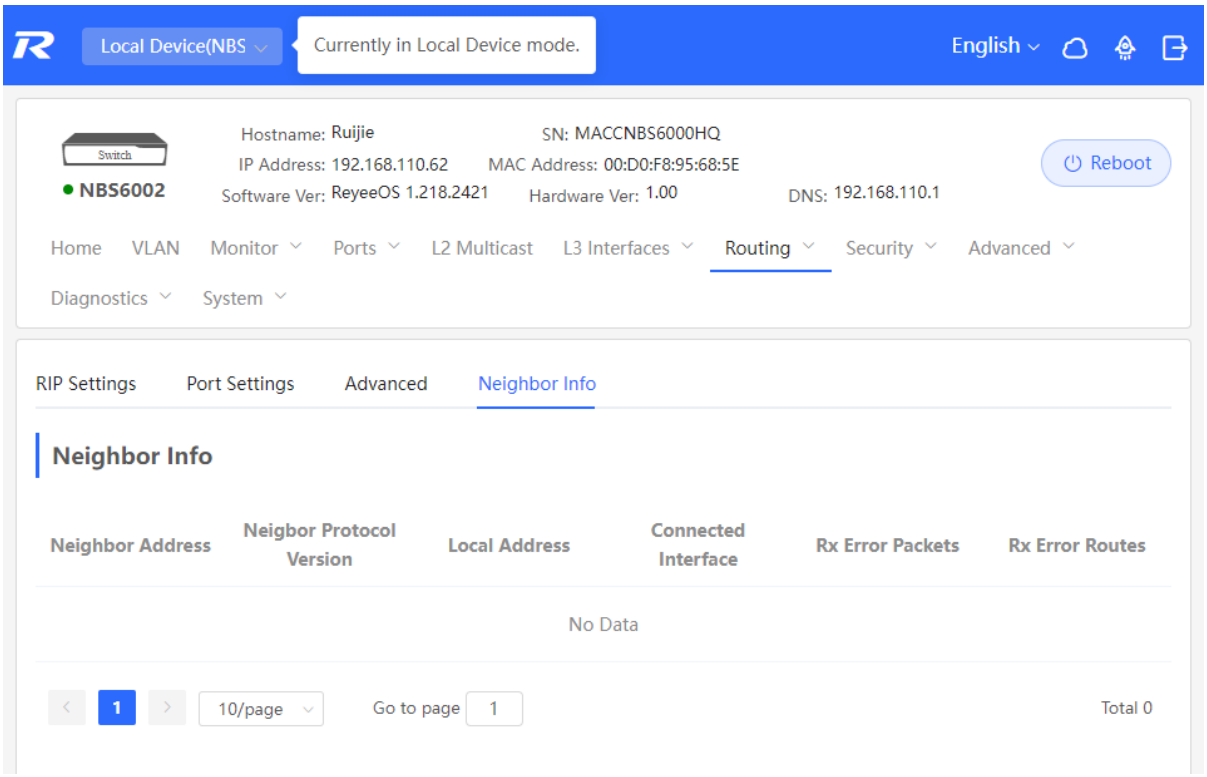


7.3.6 Configuring the Neighbor Route

When the router cannot process broadcast packets, another router can be designated as the neighbor to establish a RIP direct link.

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced**, click **Add**, and enter the IP address of the neighbor router.


Local Device(NBS
Currently in Local Device mode.
English
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
NBS6002
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced
Diagnostics System
Add
* Neighbor Route
Cancel
OK
Type
Action
Passive Interface
RIP update packets will b
are advised to enable this function.
oes not adopt RIP, you
Passive Interface
+ Add
Delete Selected
Port Name
Action
No Data
Neighbor Route
If a router cannot forward broadcast packets, another router is designated as the neighbor to establish a RIP direct link.
Neighbor Route
+ Add
Delete Selected
Address
Action
No Data



7.4 Configuring RIPng

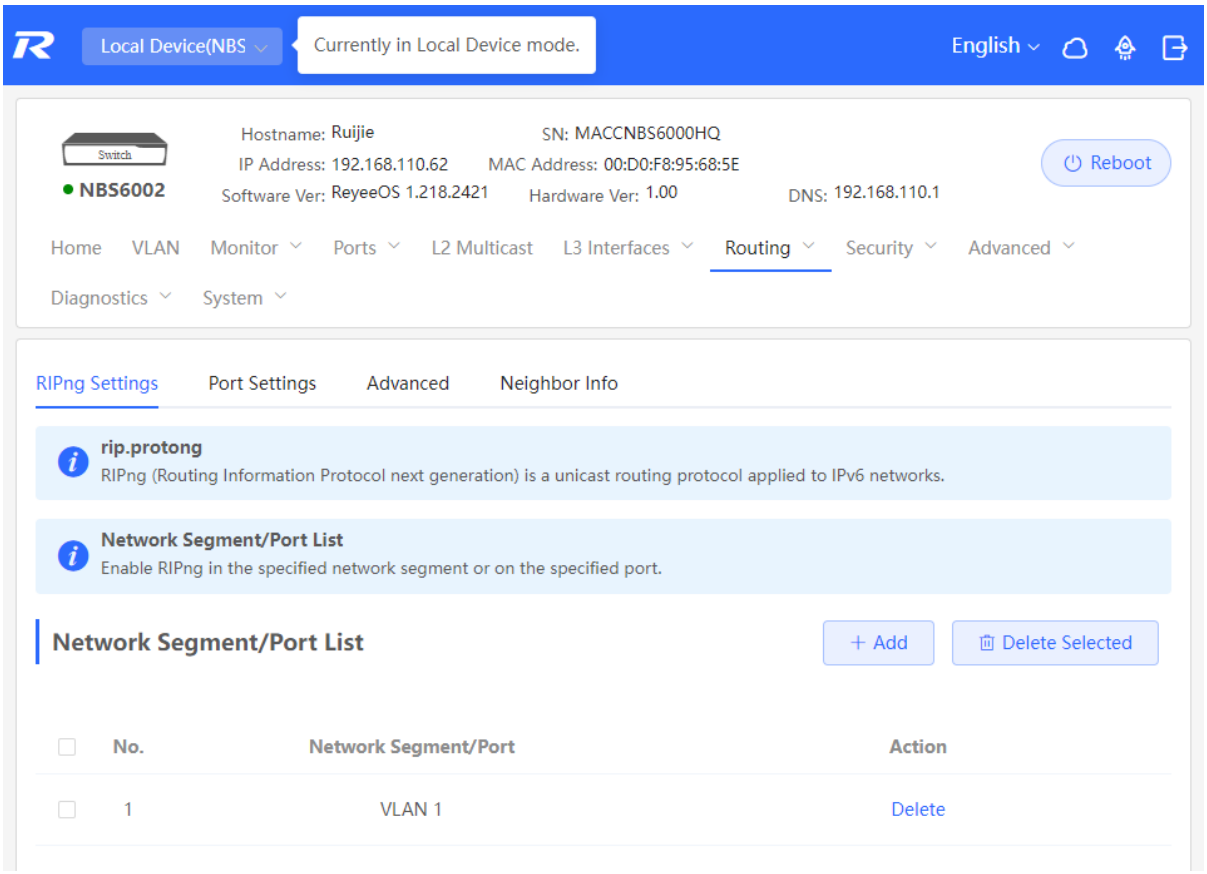
7.4.1 Configuring RIPng Basic Functions

RIP Next Generation (RIPng) provides the routing function for IPv6 networks.

RIPng uses UDP port 512 to exchange the routing information.

Choose **Local Device** > **Routing** > **RIPng Settings**.

Click **Add**, set **Type** to **Network Segment** or **Port**, and specify the network segment or port accordingly.

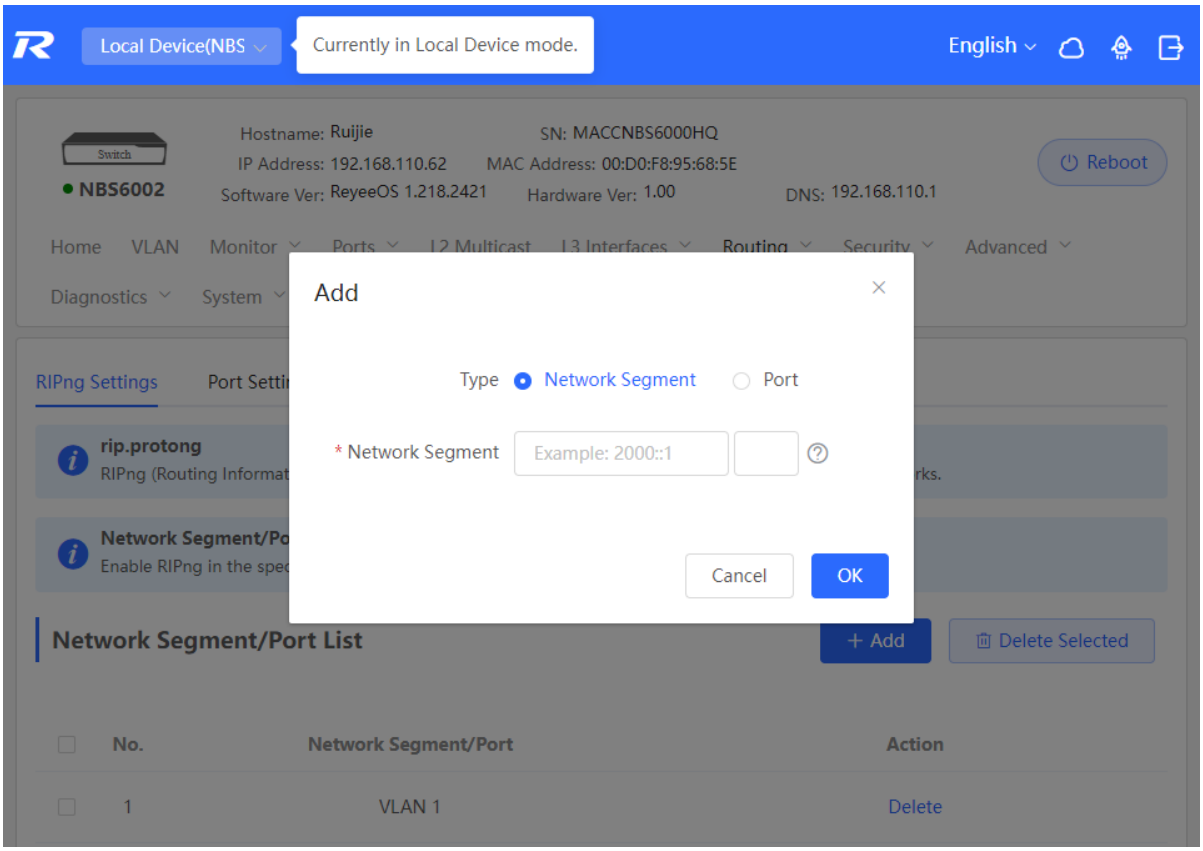


rip.protong

RIPng (Routing Information Protocol next generation) is a unicast routing protocol applied to IPv6 networks.

Network Segment/Port List

Enable RIPng in the specified network segment or on the specified port.



If the address length is between 48 and 64, the address will be used as a prefix.

Alternatively, enable RIPng on a specified port:

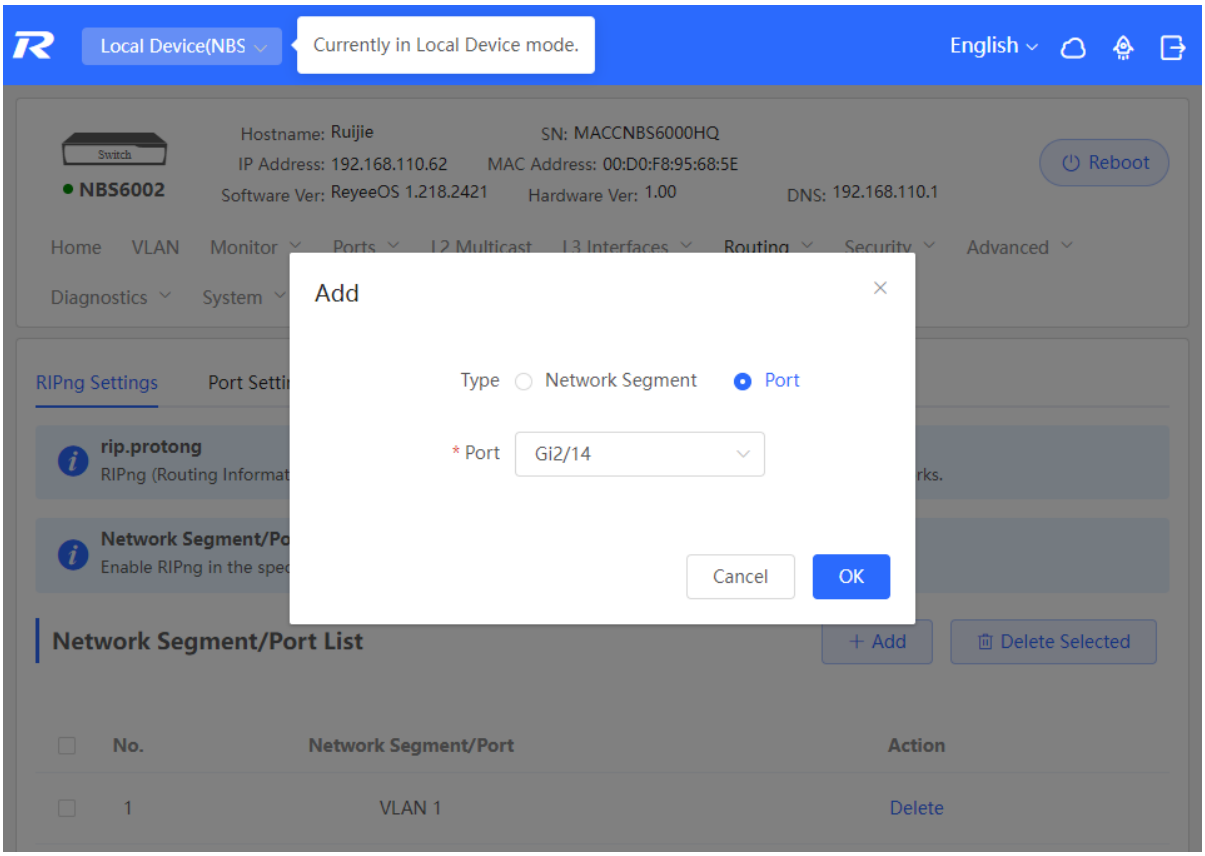


Table 7-7 RIPng Configuration Parameters

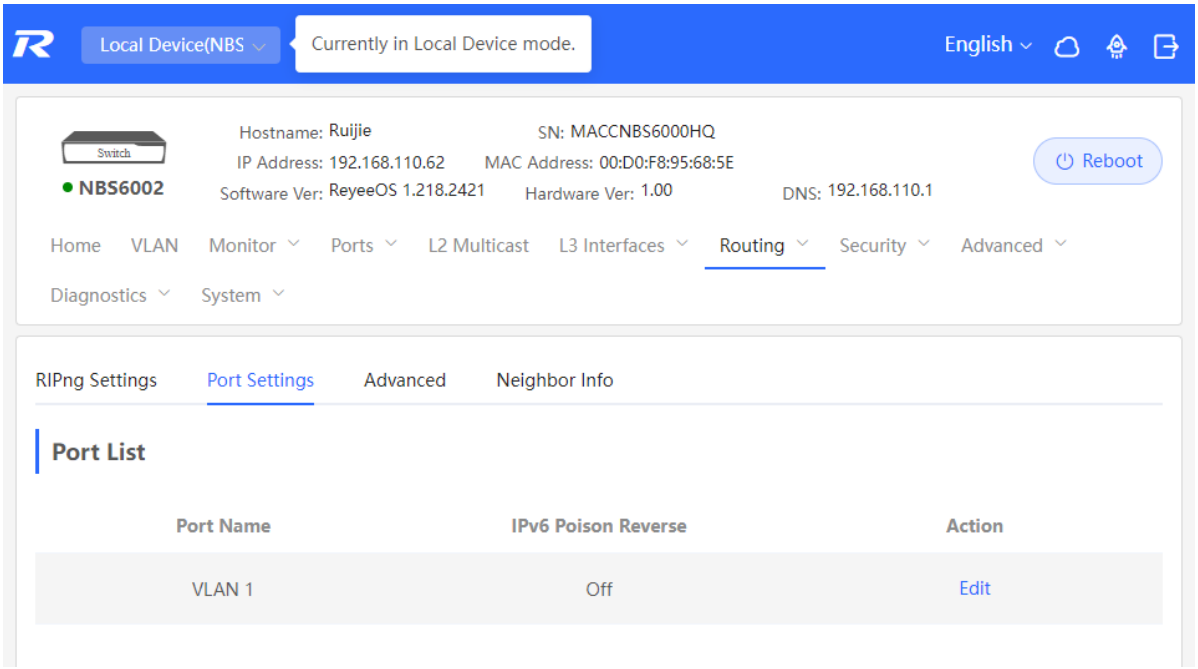
Parameter	Description
Type	**Network Segment**: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other. **Port**: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.
Network Segment	Enter the IPv6 address and prefix length when **Type** is set to **Network Segment**. RIPng will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when **Type** is

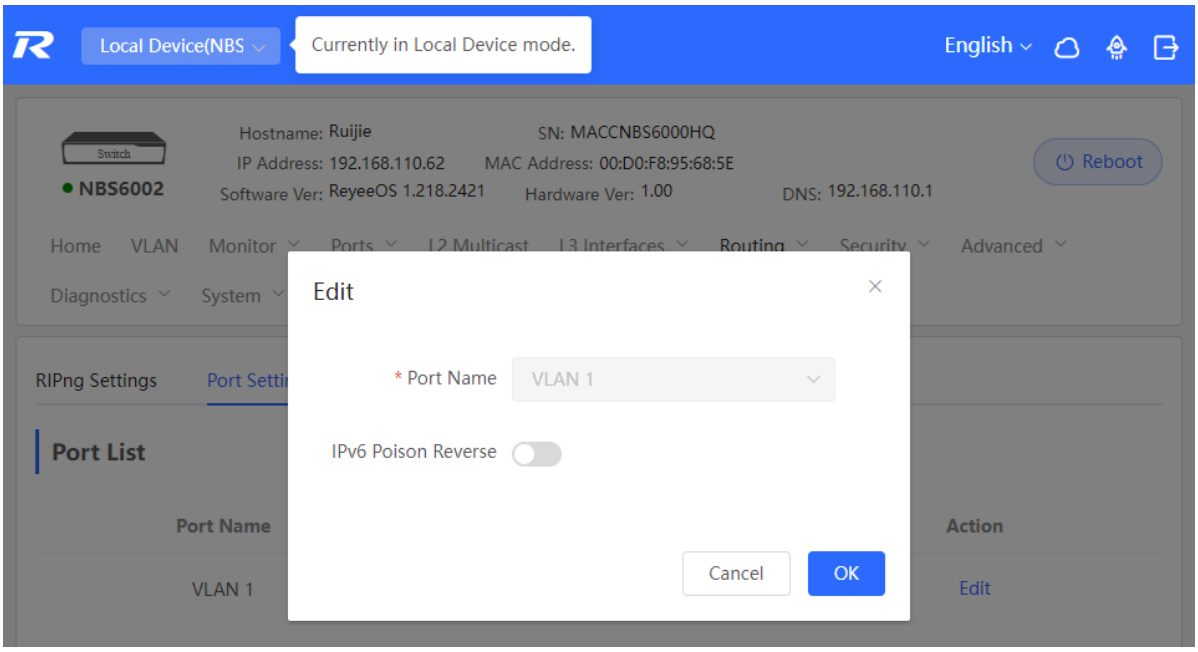
	set to **Port**.

7.4.2 Configuring the RIPng Port

RIPng poison reverse: After the port learns the route, the route overhead is set to **16** (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.

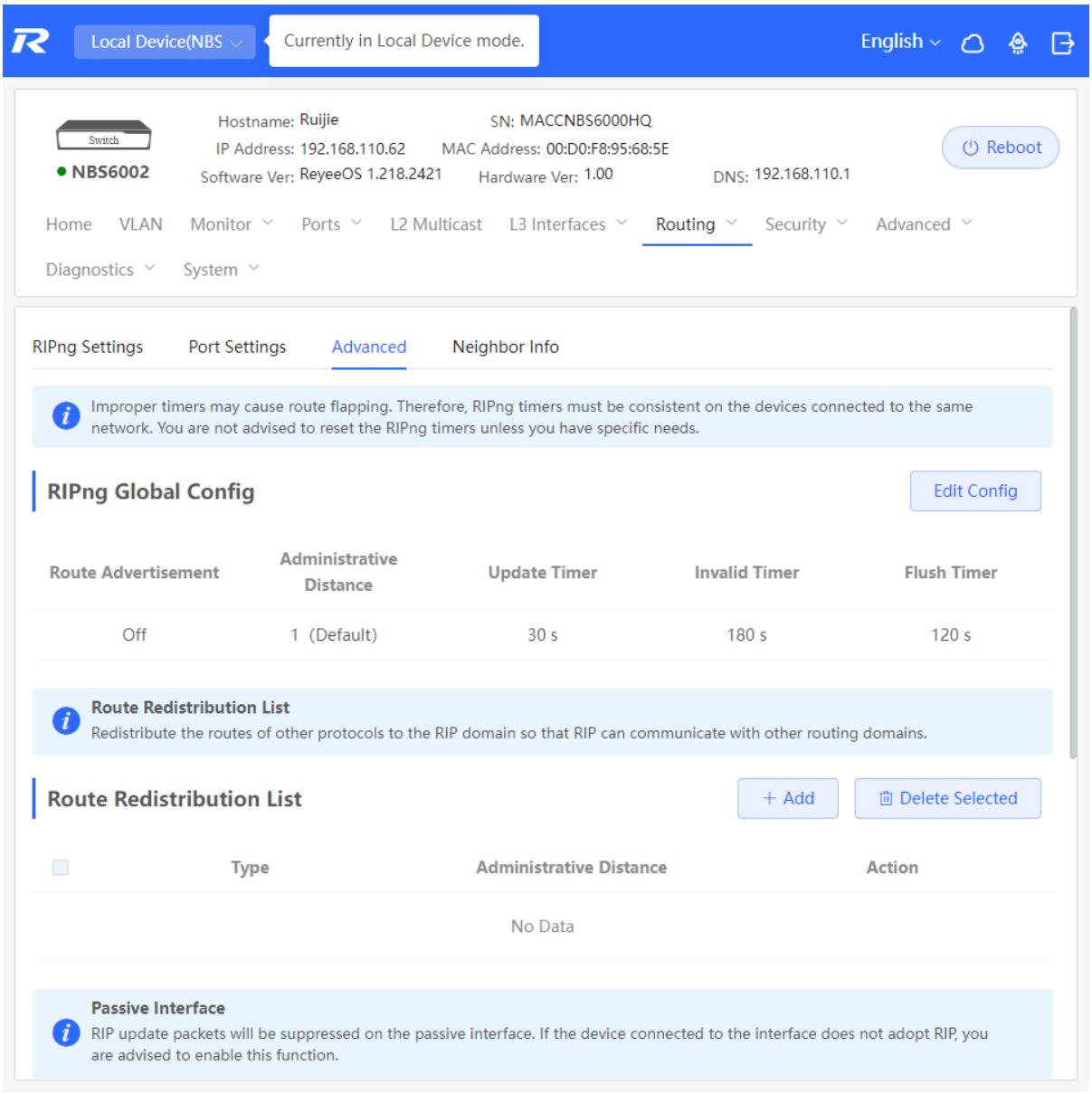
Choose **Local Device** > **Routing** > **RIPng Settings** > **Port Settings**, click Edit, and enable IPv6 poison reverse.





7.4.3 Configuring the RIPng Global Configuration

Choose **Local Device** > **Routing** > **RIPng Settings** > **Advanced**, and click **Edit Config**.


Local Device(NBS
Currently in Local Device mode.
English
Switch
NBS6002
Hostname: Ruijie
SN: MACCNBS6000HQ
IP Address: 192.168.110.62
MAC Address: 00:D0:F8:95:68:5E
Software Ver: ReyeeOS 1.218.2421
Hardware Ver: 1.00
DNS: 192.168.110.1
Reboot
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Interfaces
Routing
Security
Advanced
Diagnostics
System
RIPng Settings
Port Settings
Advanced
Neighbor Info
Improper timers may cause route flapping. Therefore, RIPng timers must be consistent on the devices connected to the same network. You are not advised to reset the RIPng timers unless you have specific needs.
RIPng Global Config
Edit Config
Route Advertisement
Administrative Distance
Update Timer
Invalid Timer
Flush Timer
Off
1 (Default)
30 s
180 s
120 s
Route Redistribution List
Redistribute the routes of other protocols to the RIP domain so that RIP can communicate with other routing domains.
Route Redistribution List
+ Add
Delete Selected
Type
Administrative Distance
Action
No Data
Passive Interface
RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

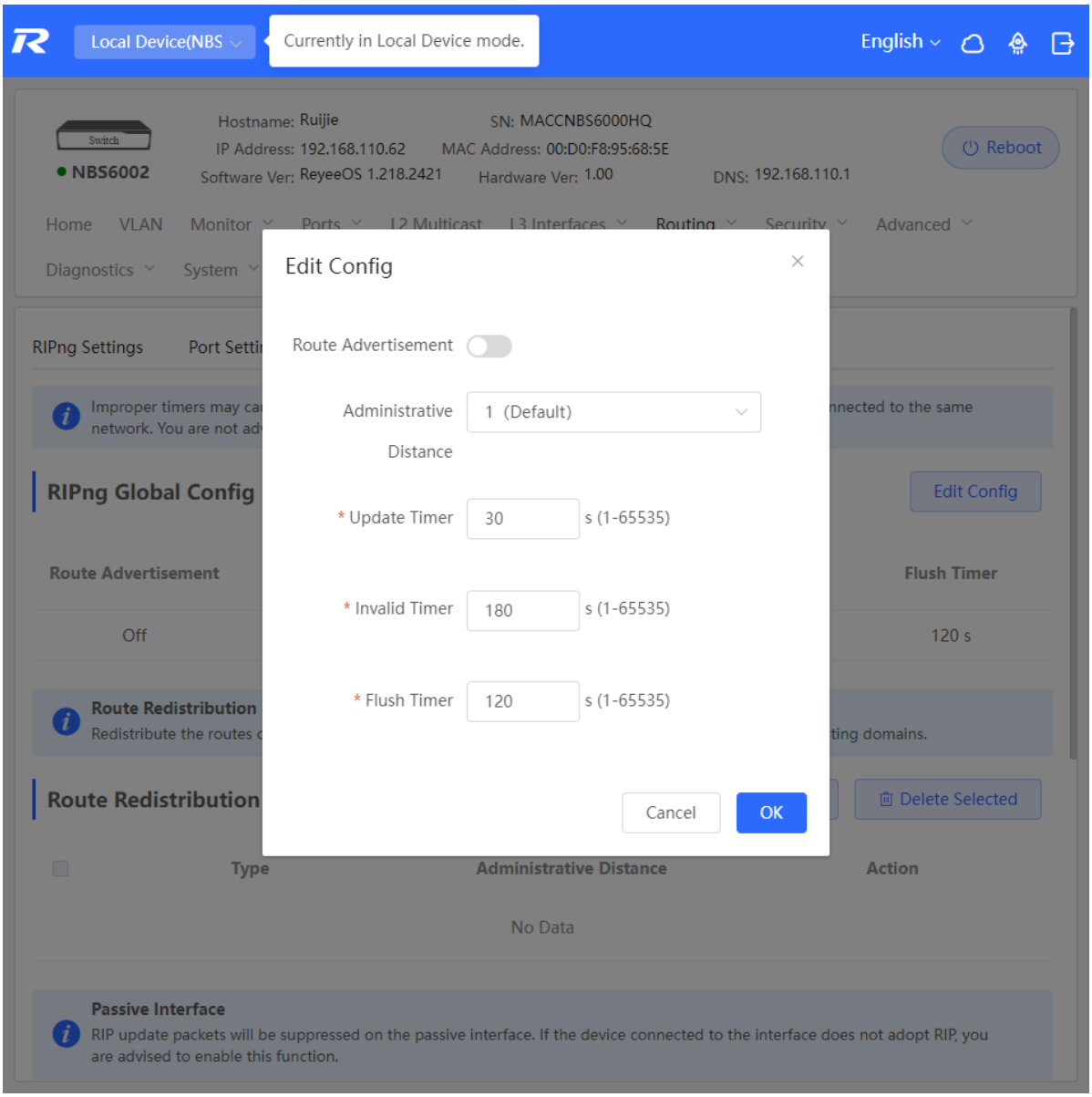


Table 7-8 RIPng Global Configuration Parameters

Parameter	Description
Route Advertisement	After route advertisement is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.

Parameter	Description
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

7.4.4 Configuring the RIPng Route Redistribution List

Redistribute routes of other protocols to the RIPng domain to interwork with other routing domains.

Choose **Local Device** > **Routing** > **RIPng Settings** > **Advanced**, and click **+ Add**.

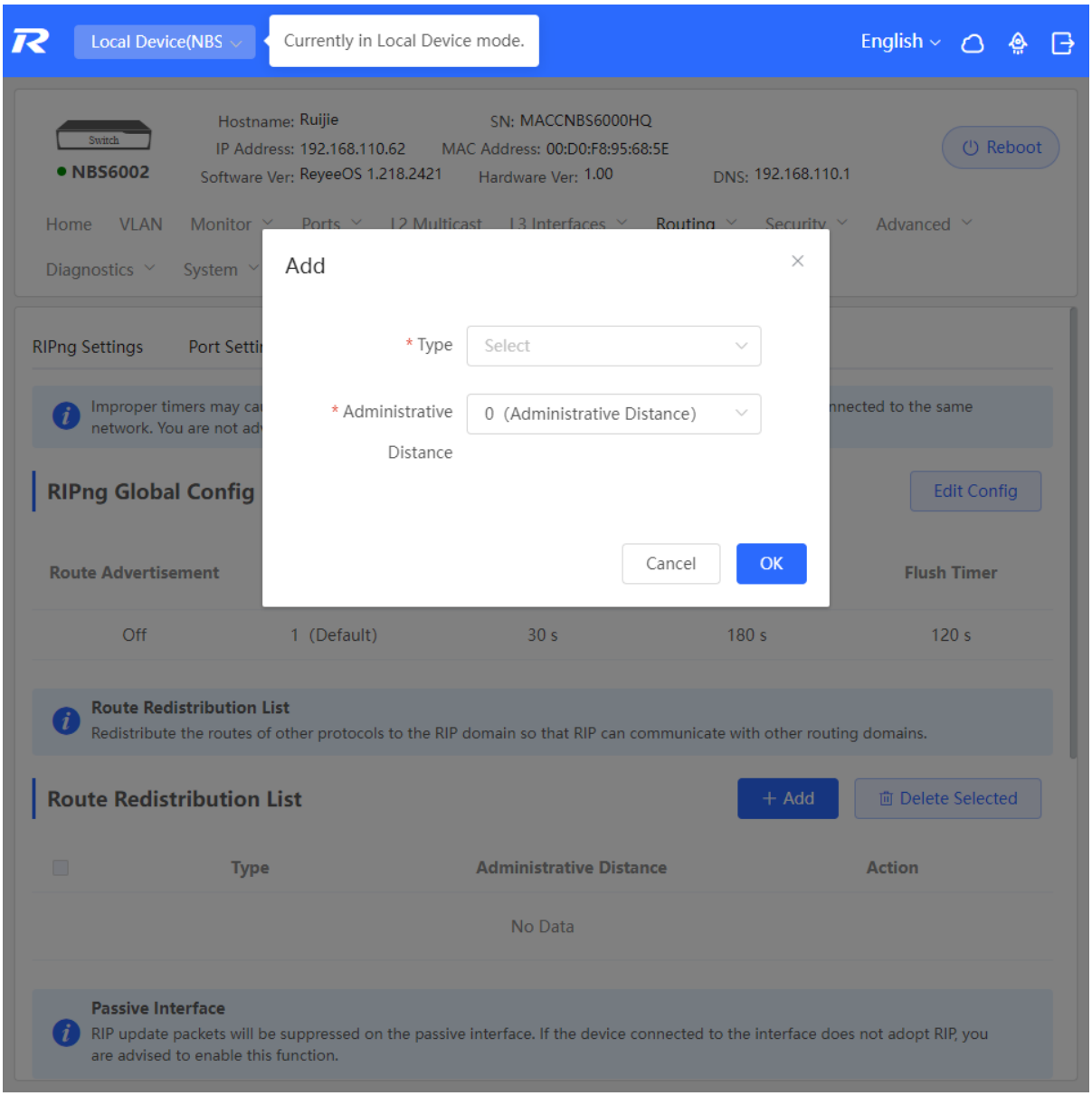


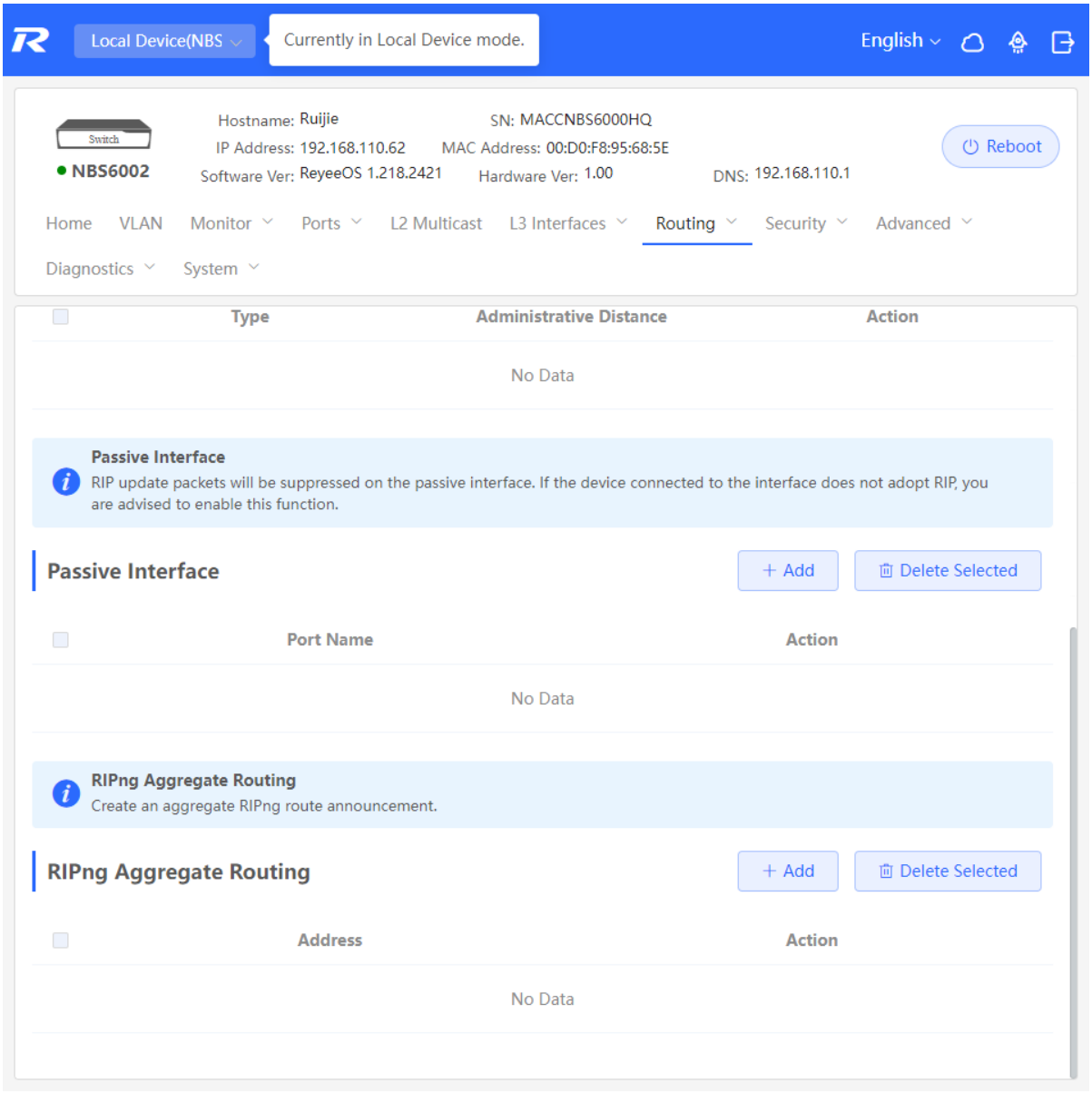
Table 7-9 RIP Route Redistribution Parameters

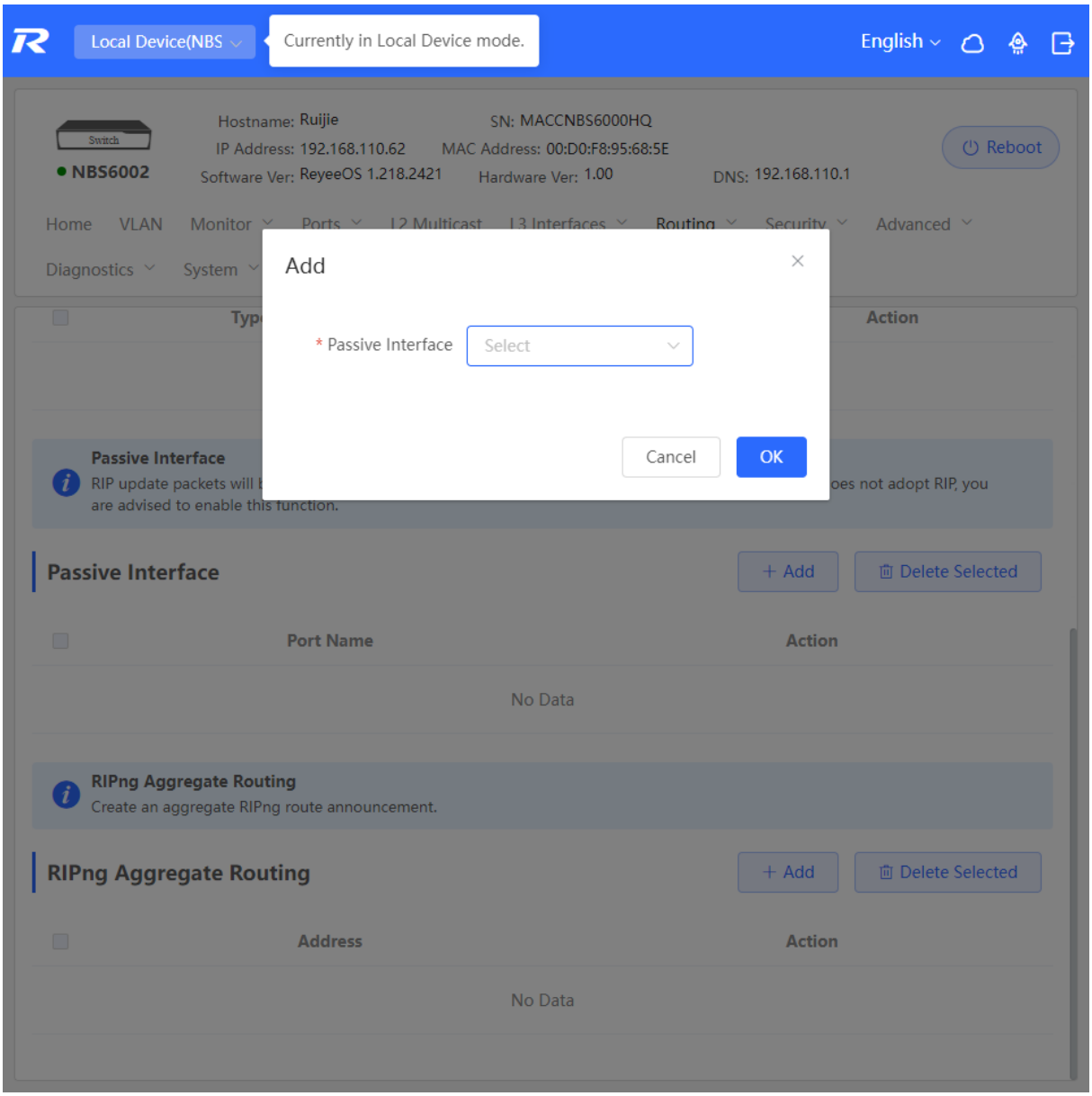
Parameter	Description
Type	Direct Routing OSPF Routing Static Routing
Administrative Distance	Value range: 0-16. The default value is **0**.

7.4.5 Configuring the RIPng Passive Interface

If an interface is configured as a passive interface, it will suppress RIPng update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

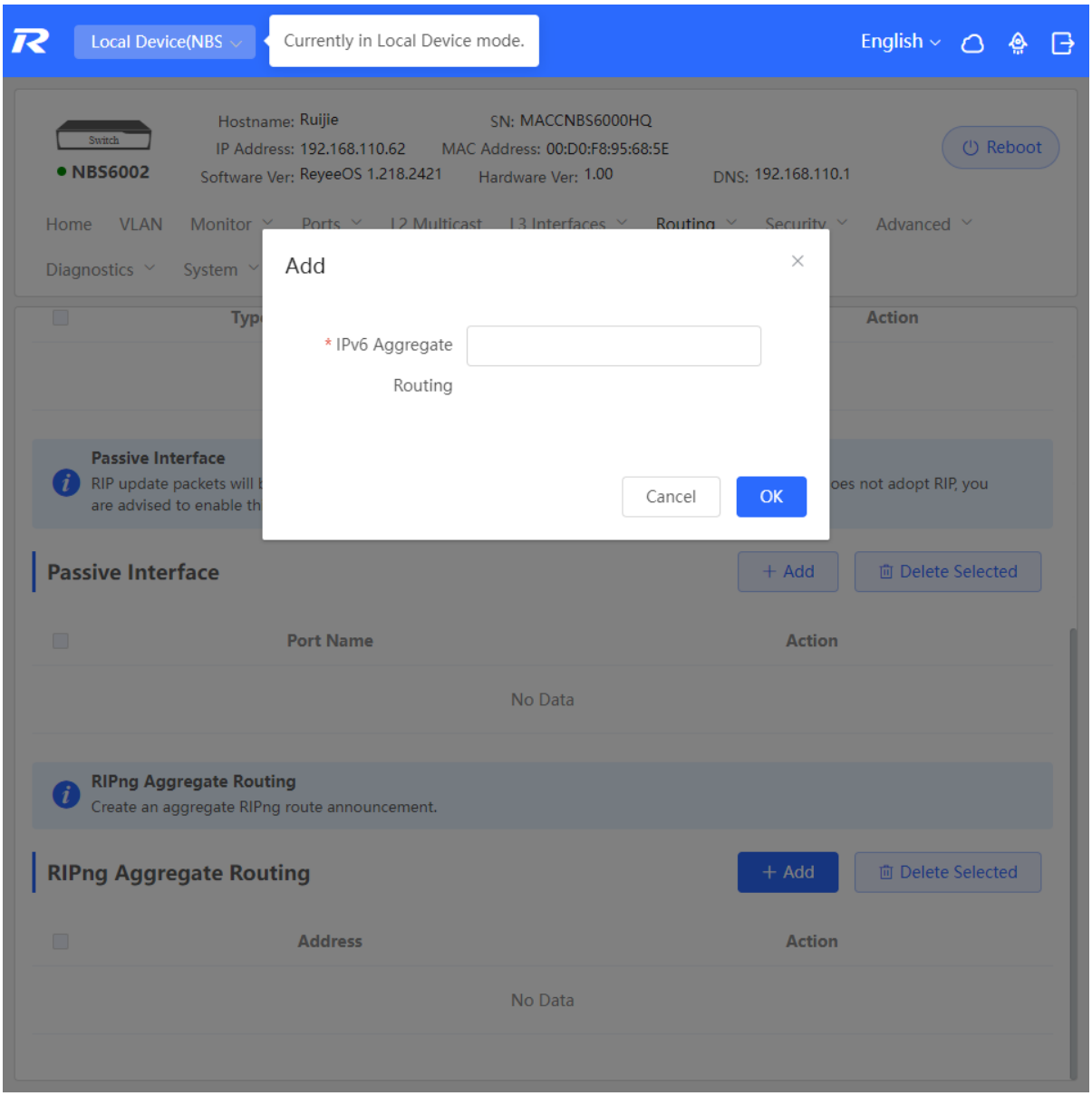
Choose **Local Device** > **Routing** > **RIPng Settings** > **Advanced**, click **Add**, and enter the IP address of the neighbor router.





7.4.6 Configuring the IPv6 Aggregate Route

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced**, click **Add**, and enter the IPv6 address and prefix length (value range: 0 to 128).



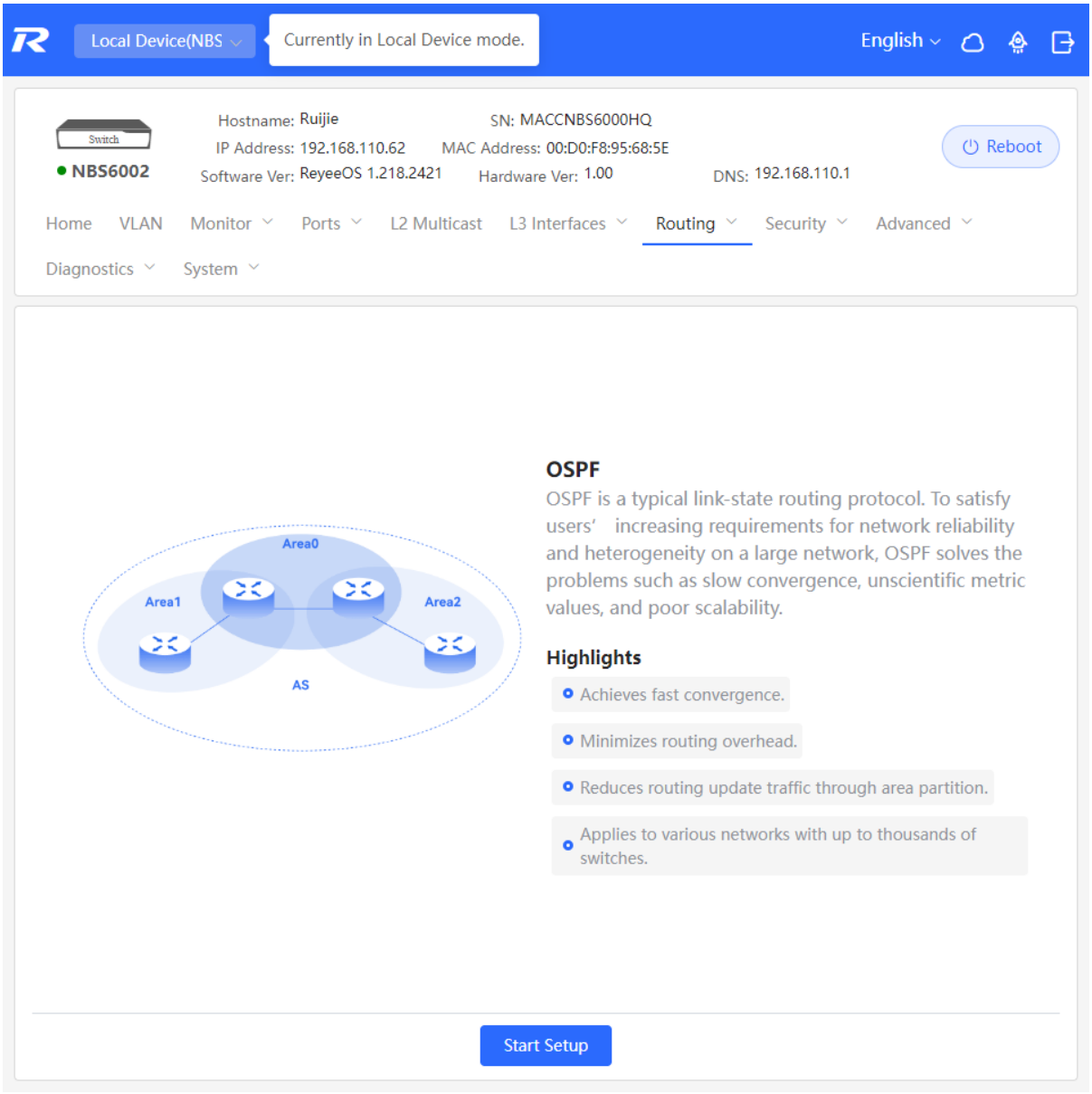
7.5 OSPFv2

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

OSPF is a typical link-state routing protocol, which can solve the problems of slow route update, inaccurate measurement, and poor scalability in large networks. It is suitable for networks of various sizes, and even a network with up to thousands of devices.

7.5.1 Configuring OSPFv2 Basic Parameters

Choose **Local Device** > **Routing** > **OSPFv2**, click **Start Setup**, and then configure an instance and an interface respectively.



(1) Configure an instance.

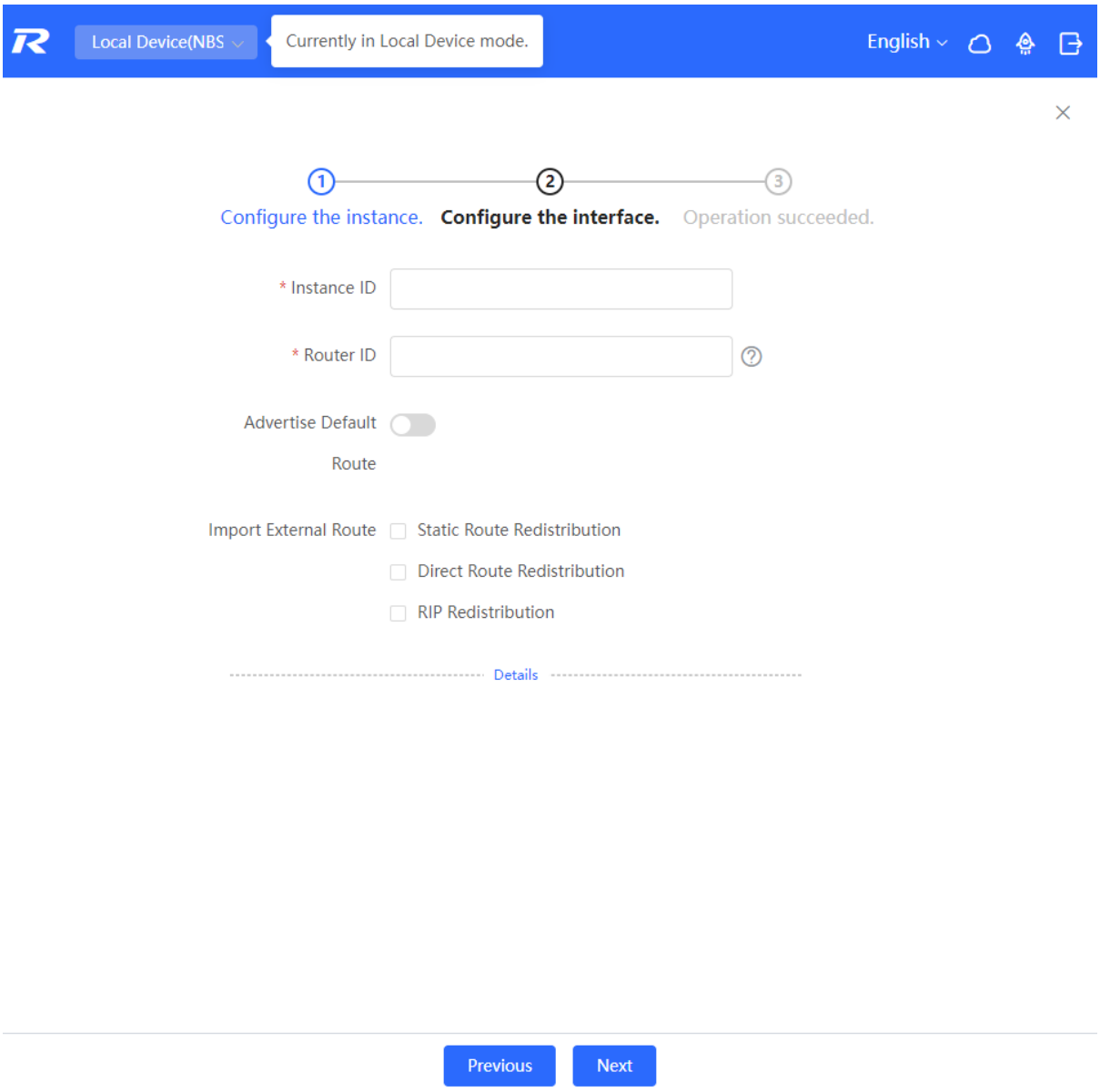


Table 7-10 Instance Configuration Parameters

Parameter	Description
Instance ID	Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices.
Router ID	It identifies a router in an OSPF domain. **Caution** Router IDs within the same domain must be unique. The same configuration may cause

Parameter	Description
	neighbor discovery failures.
Advertise Default Route	Generate a default route and send it to the neighbor. After this function is enabled, you need to enter the metric and select a type. The default metric is **1**. Type 1: The metrics displayed on different routers vary. Type 2: The metrics displayed on all routers are the same.
Import External Route	Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains. If **Static Route Redistribution** is selected, enter the metric, which is **20** by default. If **Direct Route Redistribution** is selected, enter the metric, which is **20** by default. If **RIP Redistribution** is selected, enter the metric, which is **20** by default.
Details	Expand the detailed configuration.

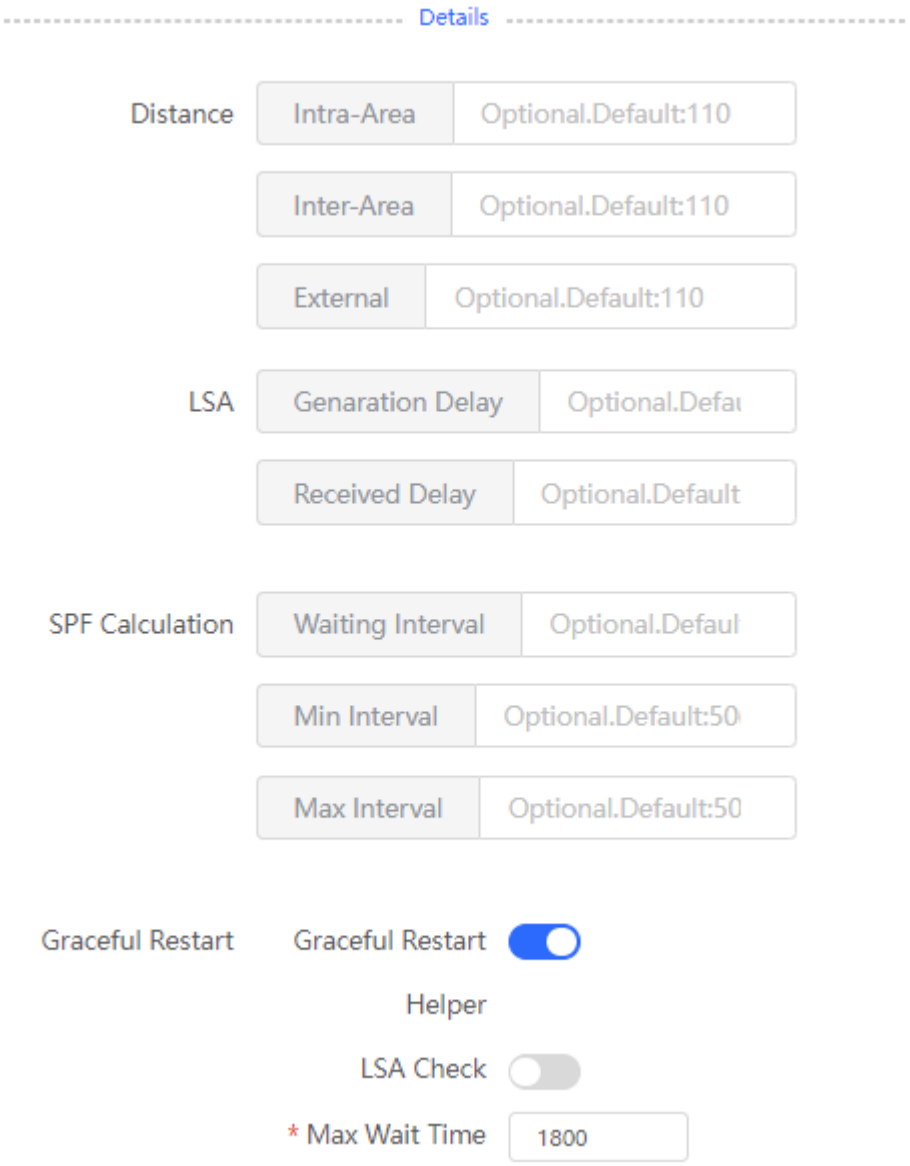


Table 7-11 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all **110**.
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default.

Parameter	Description
	The default value is 1000 ms.
SPF Calculation	When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources **Waiting Interval**: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. **Min Interval**: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. **Max Interval**: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.
Graceful Restart	Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services. **Graceful Restart Helper**: The Graceful Restart Helper function is enabled when this switch is turned on. **LSA Check**: LSA packets outside the domain are checked when this switch is turned on. **Max Wait Time**: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within **Max Wait Time**, the device exits the GR Helper mode. The default value is 1800 seconds.

(2) **Configure an interface.**

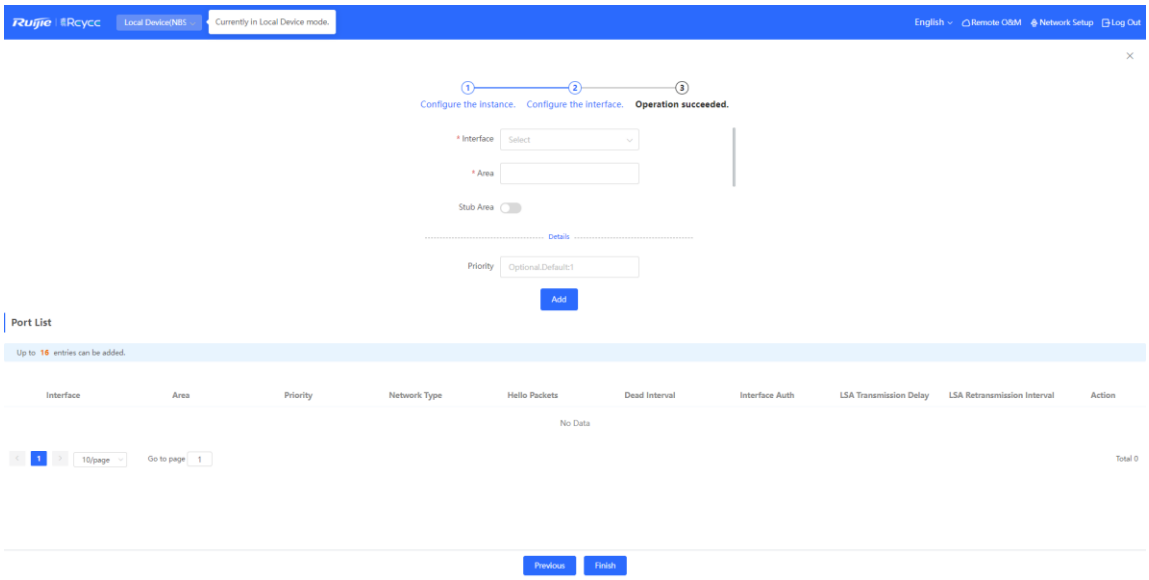


Table 7-12 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295
Stub Area	If **Stub Area** is enabled, you need to configure the area type and inter-area route isolation. Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small. Not-So-Stubby Area (NSSA): A few external routes can be imported. Inter-area route isolation: After this function is enabled, inter-area routes will not be imported to this area.
Details	Expand the detailed configuration.

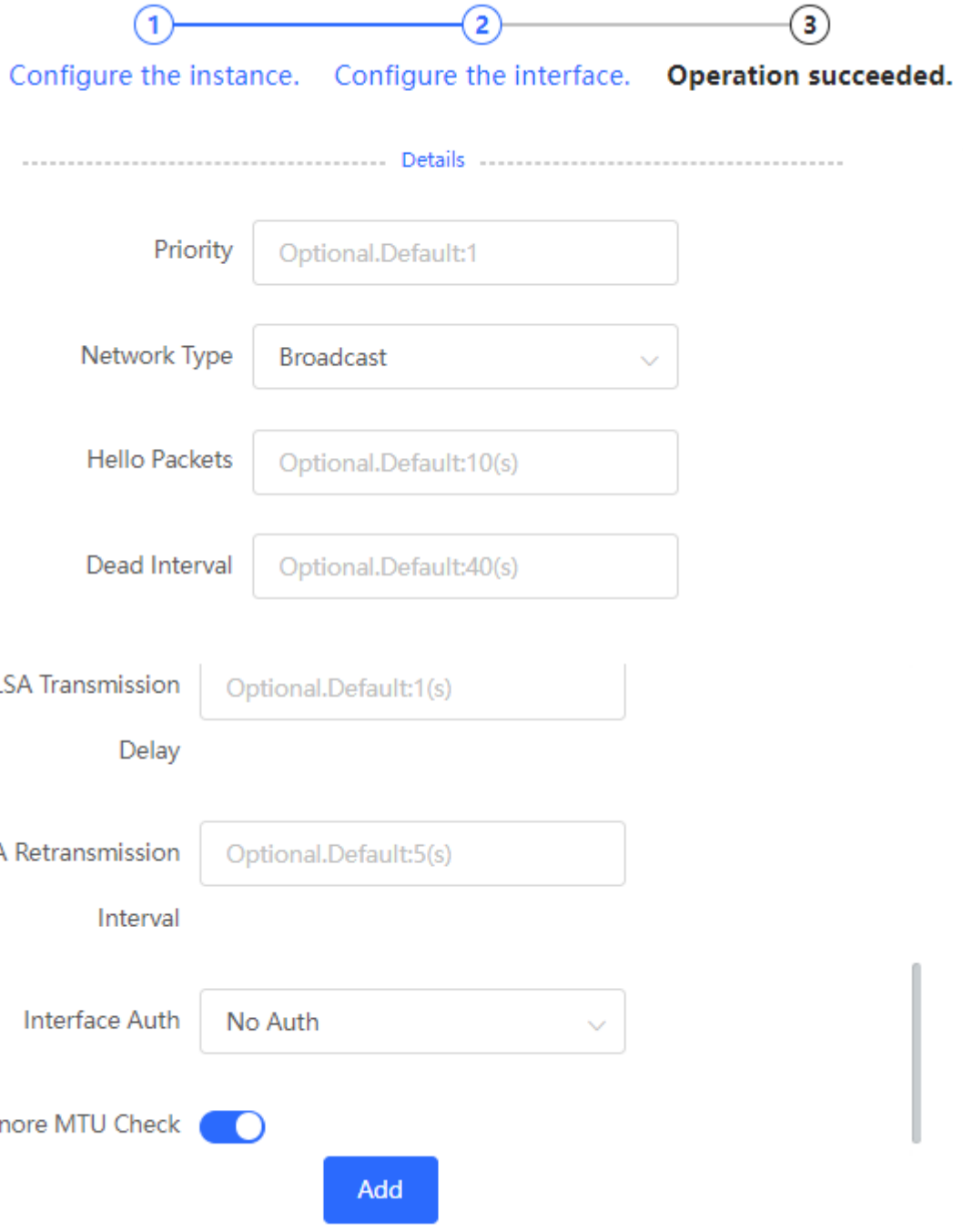


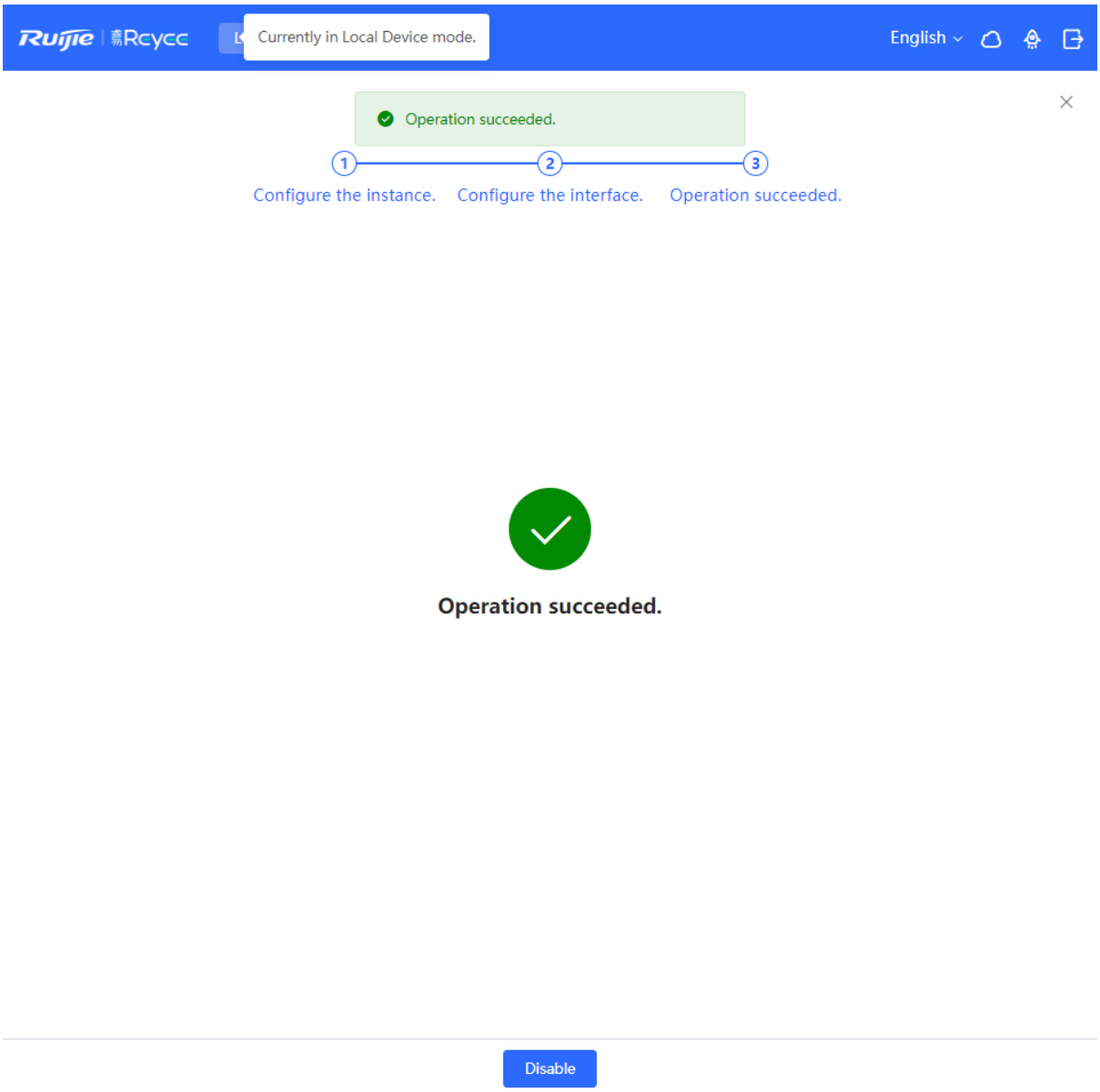
Table 7-13 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
Network Type	Broadcast

Parameter	Description
	Unicast Multicast Non-Broadcast Multiple Access
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	**No Auth**: The protocol packets are not authenticated. It is the default value. **Plain Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. **MD5**: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

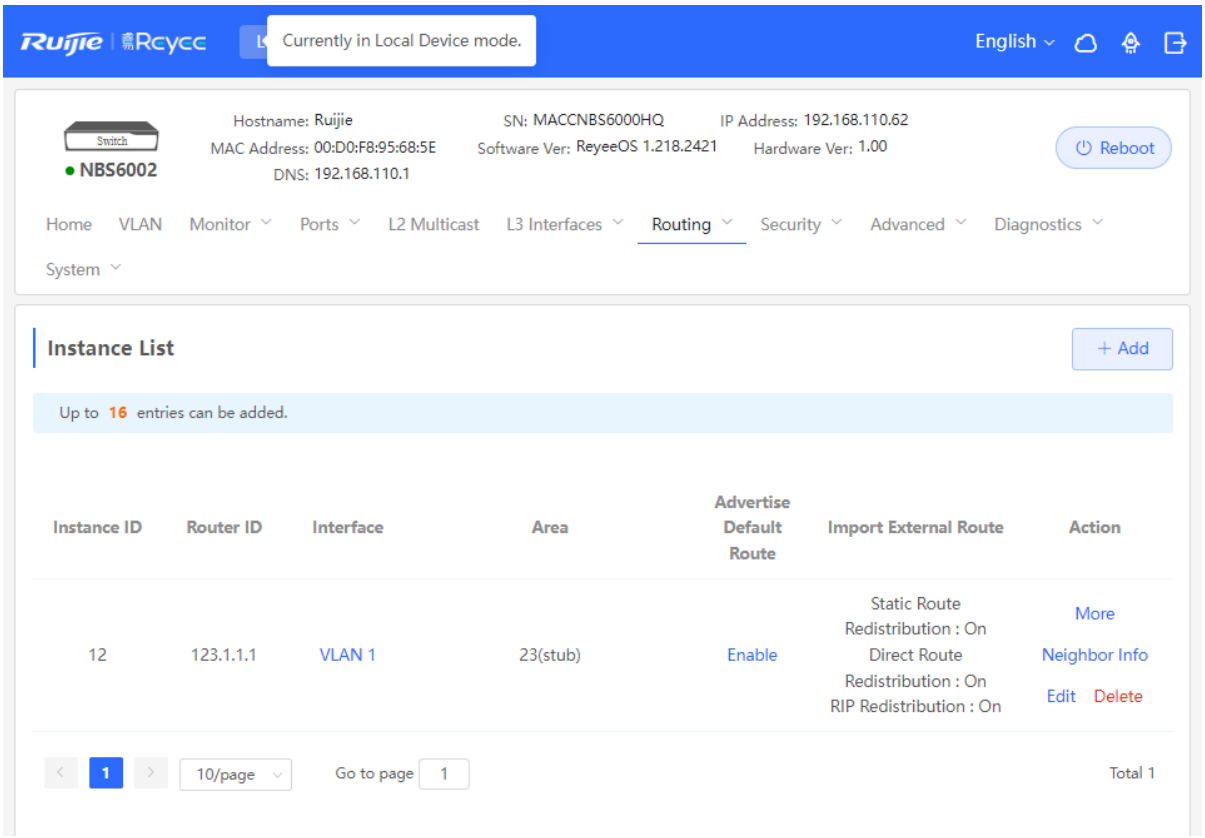
(2) Complete the configuration.

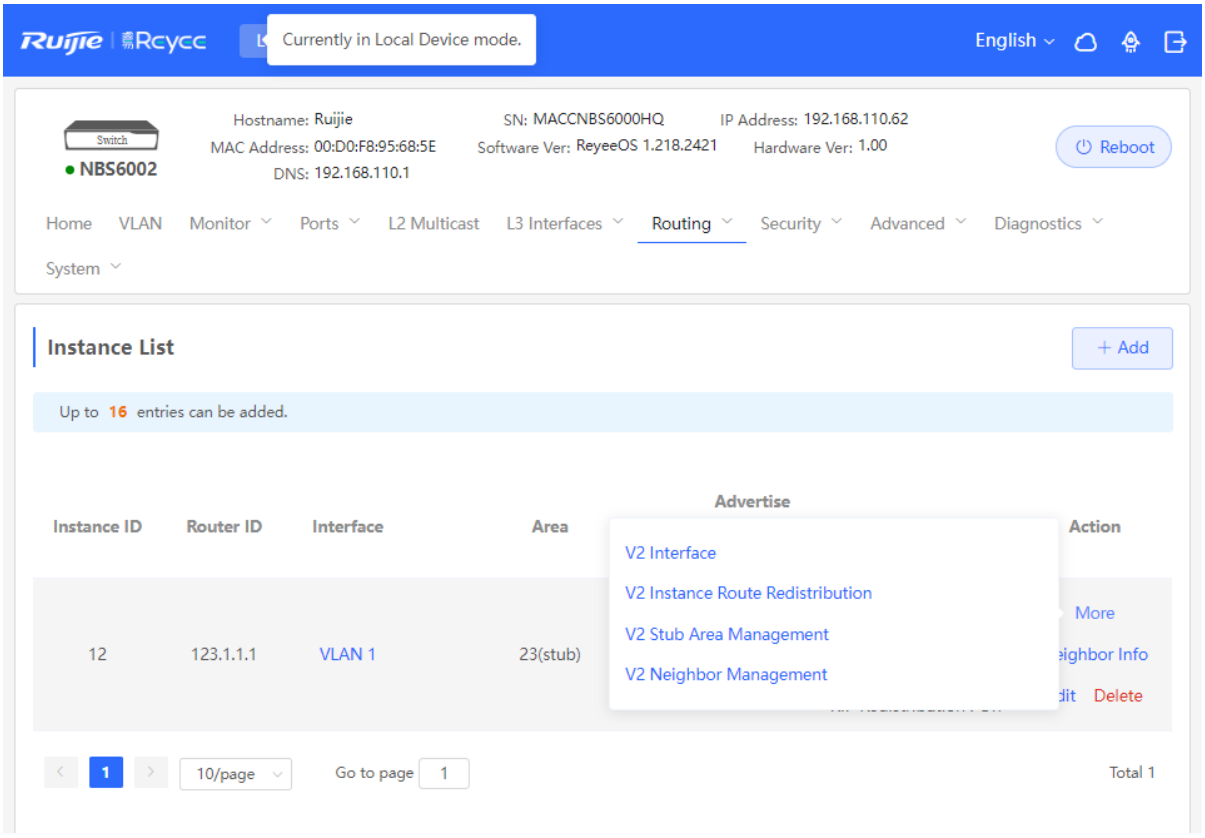
After completing the configuration, you can choose **Local Device** > **Routing** > **OSPFv2** and view the instance list.

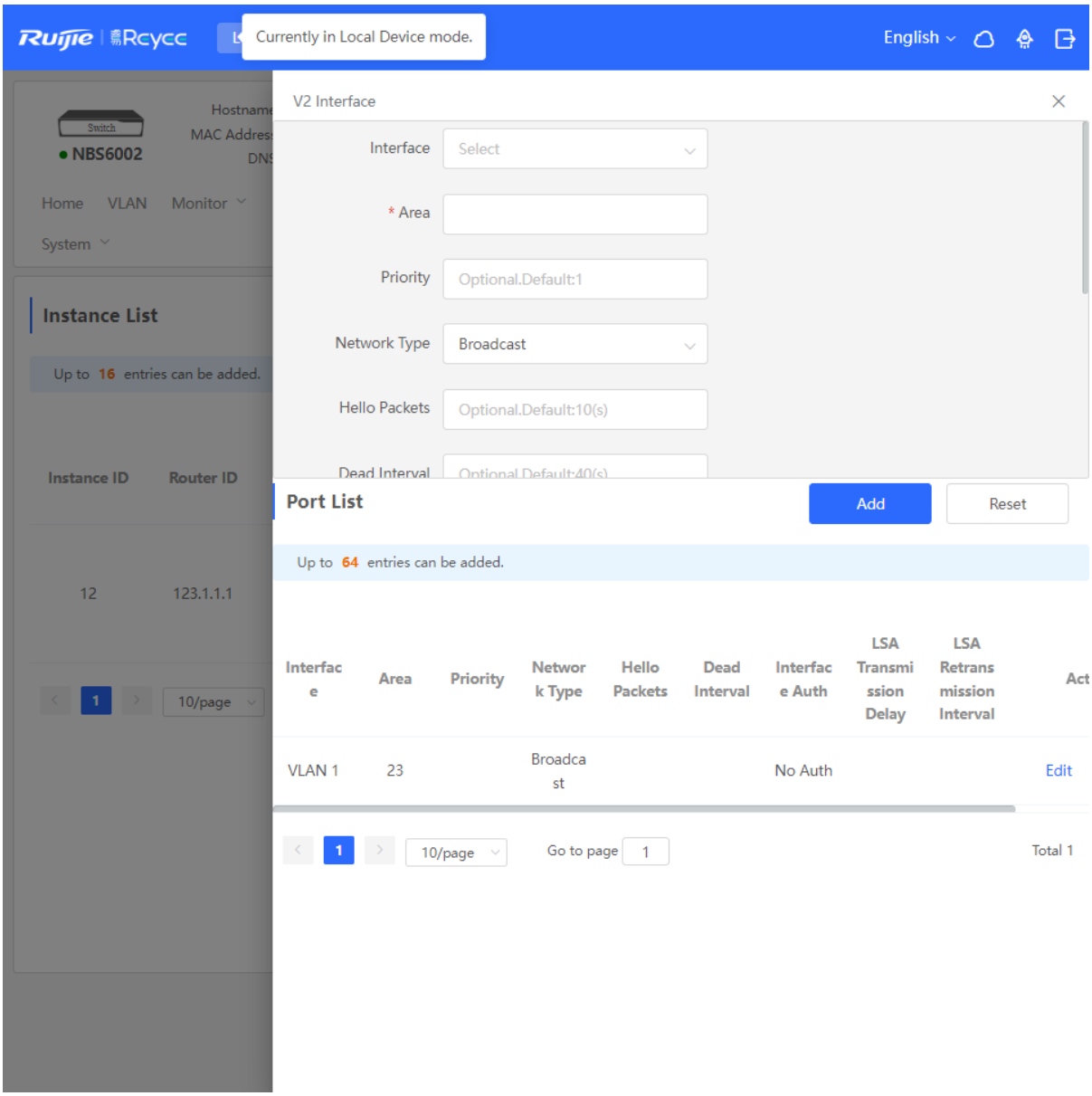


7.5.2 Adding an OSPFv2 Interface

Choose **Local Device** > **Routing** > **OSPFv2**, click **More** in the **Action** column, and select **V2 Interface**.

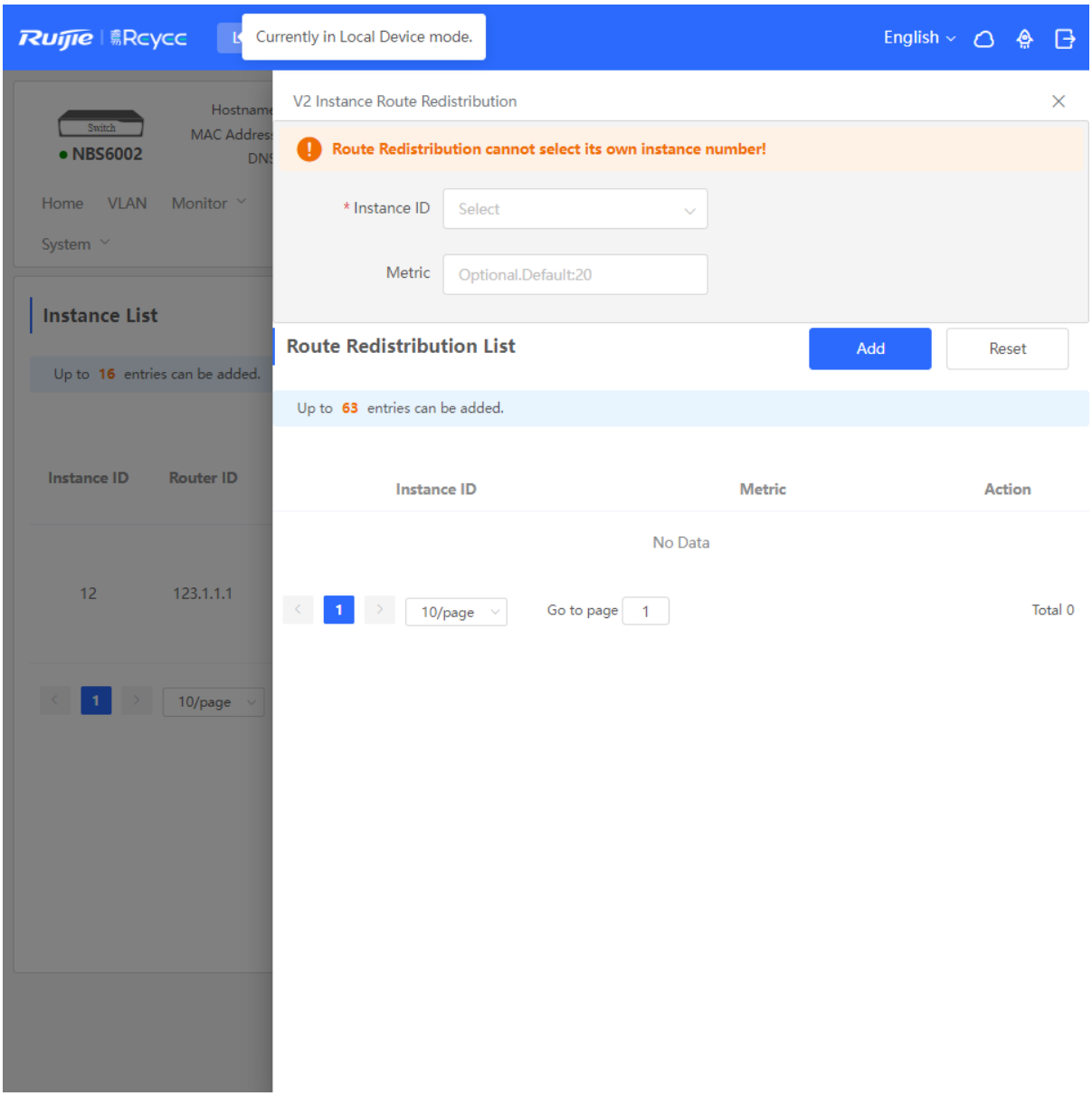

Currently in Local Device mode.
English
Hostname: Ruijie
MAC Address: 00:D0:F8:95:68:5E
DNS: 192.168.110.1
SN: MACCNBS6000HQ
Software Ver: ReyeeOS 1.218.2421
IP Address: 192.168.110.62
Hardware Ver: 1.00
NBS6002
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced Diagnostics System
Instance List
+ Add
Up to 16 entries can be added.
Instance ID Router ID Interface Area Advertise Default Route Import External Route Action
12 123.1.1.1 VLAN 1 23(stub) Enable Static Route Redistribution : On Direct Route Redistribution : On RIP Redistribution : On More Neighbor Info Edit Delete
1 10/page Go to page 1 Total 1


Currently in Local Device mode.
English
Hostname: Ruijie
MAC Address: 00:D0:F8:95:68:5E
DNS: 192.168.110.1
SN: MACCNBS6000HQ
Software Ver: ReyeeOS 1.218.2421
IP Address: 192.168.110.62
Hardware Ver: 1.00
NBS6002
Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced Diagnostics System
Instance List
+ Add
Up to 16 entries can be added.
Instance ID Router ID Interface Area Advertise Action
V2 Interface
V2 Instance Route Redistribution
V2 Stub Area Management
V2 Neighbor Management
12 123.1.1.1 VLAN 1 23(stub) More
1 10/page Go to page 1 Total 1



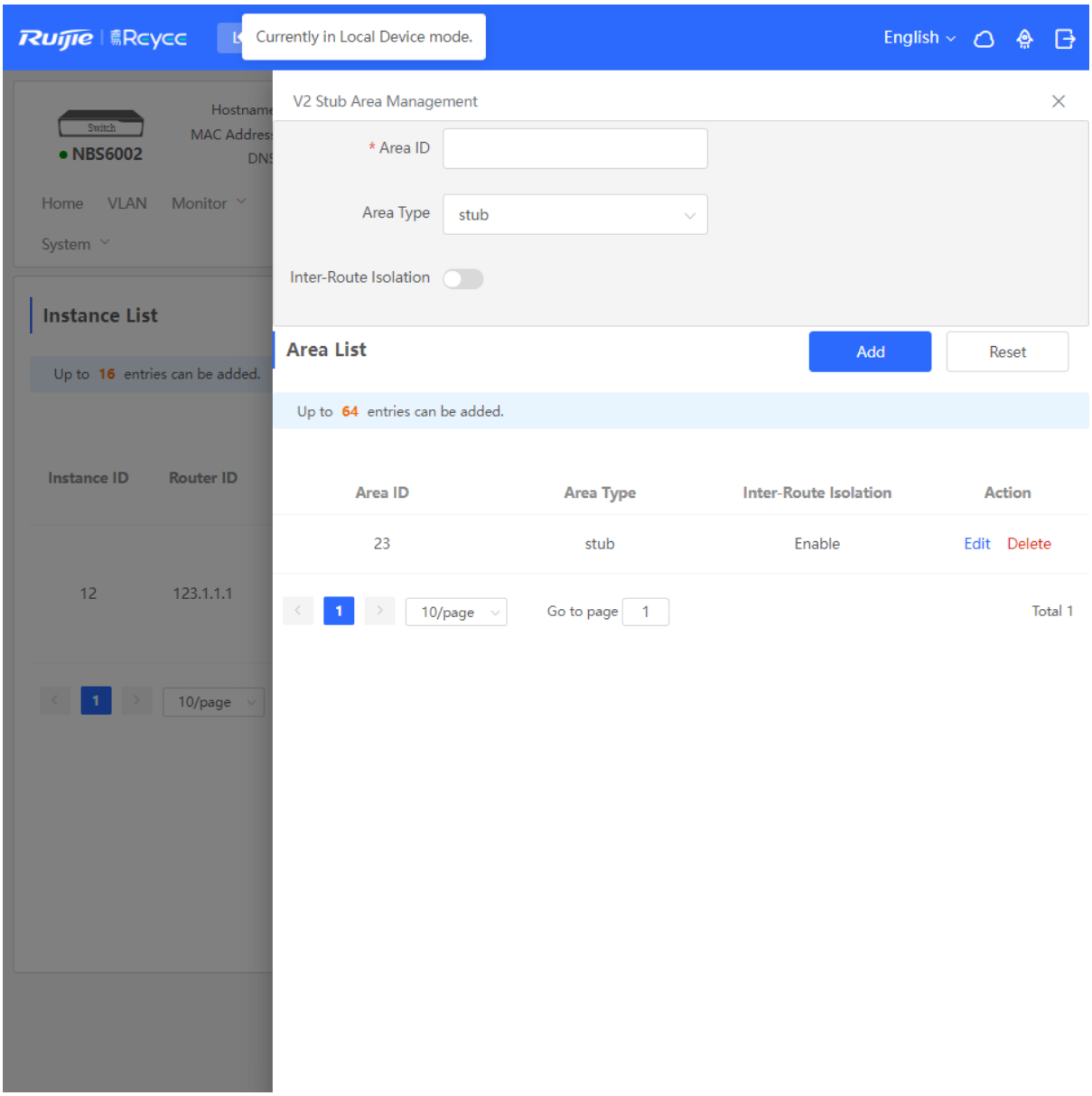
7.5.3 Redistributing OSPFv2 Instance Routes

Choose **Local Device** > **Routing** > **OSPFv2**, click **More** in the **Action** column, and select **V2 Instance Route Redistribution**.



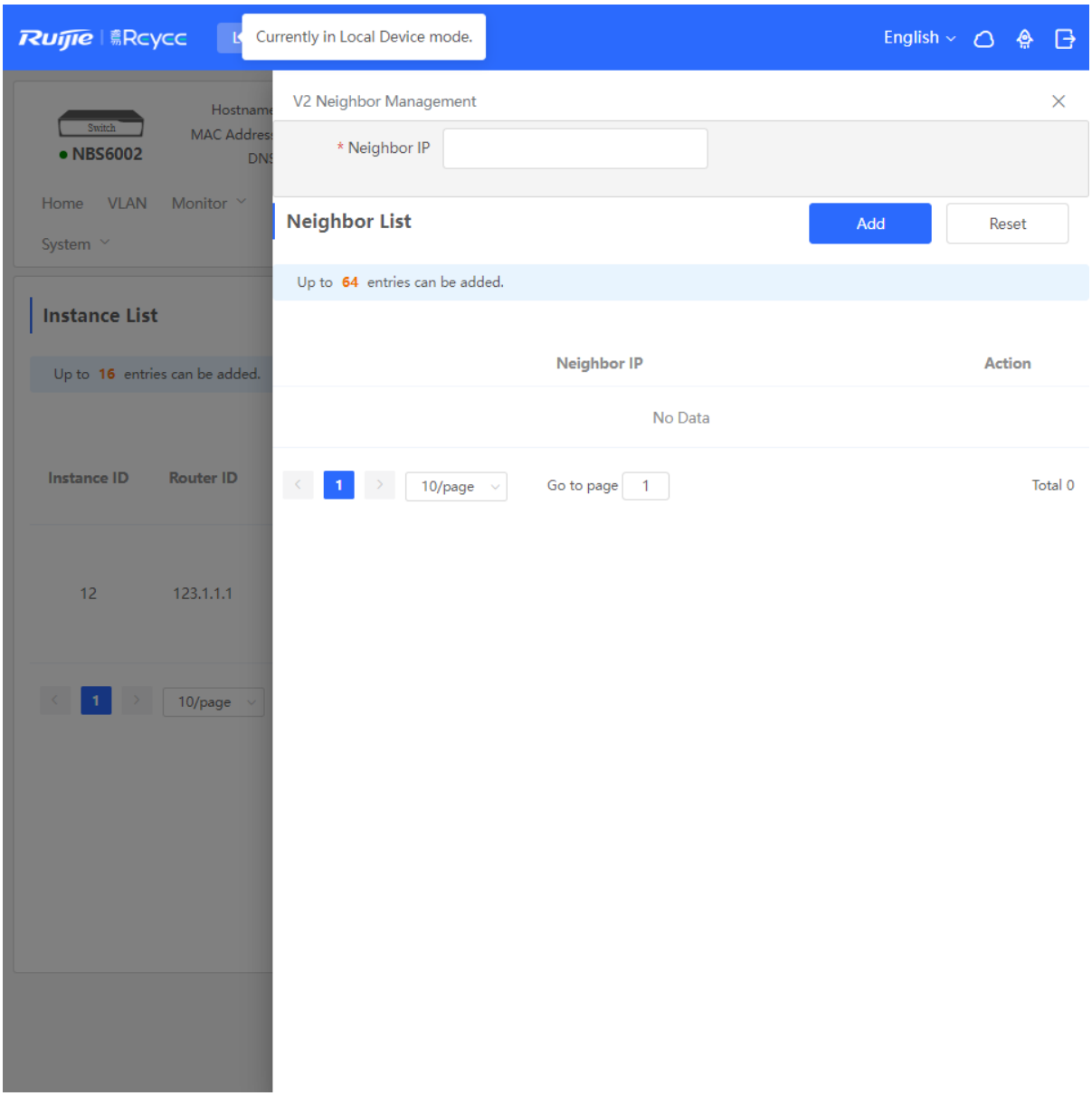
7.5.4 Managing OSPFv2 Stub Areas

Choose **Local Device** > **Routing** > **OSPFv2**, click **More** in the **Action** column, and select **V2 Stub Area Management**.



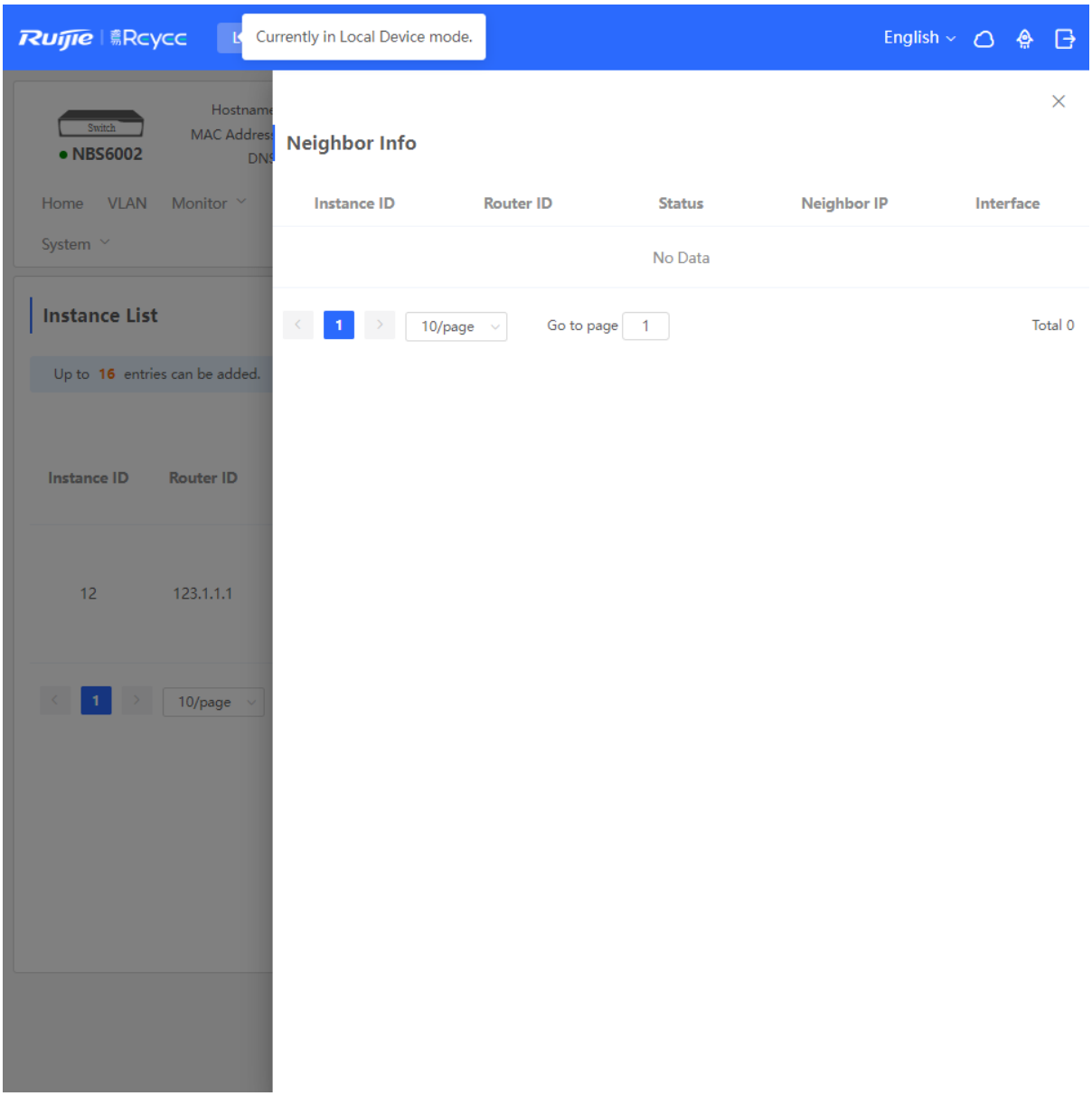
7.5.5 Managing OSPFv2 Neighbors

Choose **Local Device** > **Routing** > **OSPFv2**, click **More** in the **Action** column, and select **V2 Neighbor Management**.



7.5.6 Viewing OSPFv2 Neighbor Information

Choose **Local Device** > **Routing** > **OSPFv2**, and click **Neighbor Info** in the **Action** column.



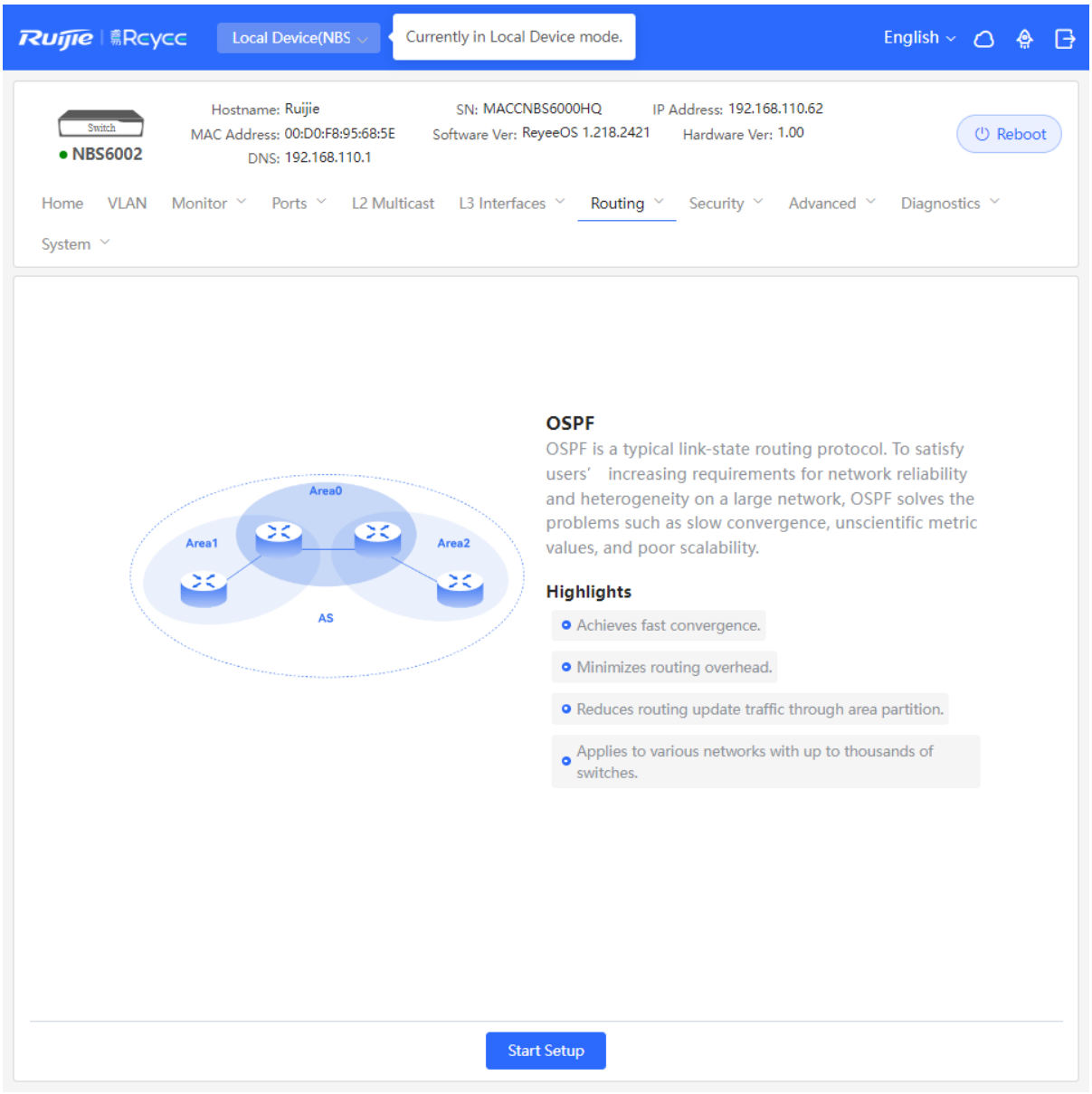
7.6 OSPFv3

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

7.6.1 Configuring OSPFv3 Basic Parameters

Choose **Local Device** > **Routing** > **OSPFv3**, click **Start Setup**, and then configure an instance and an interface respectively.

1. Configure an instance.



OSPF

OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

Highlights

Achieves fast convergence.

Minimizes routing overhead.

Reduces routing update traffic through area partition.

Applies to various networks with up to thousands of switches.

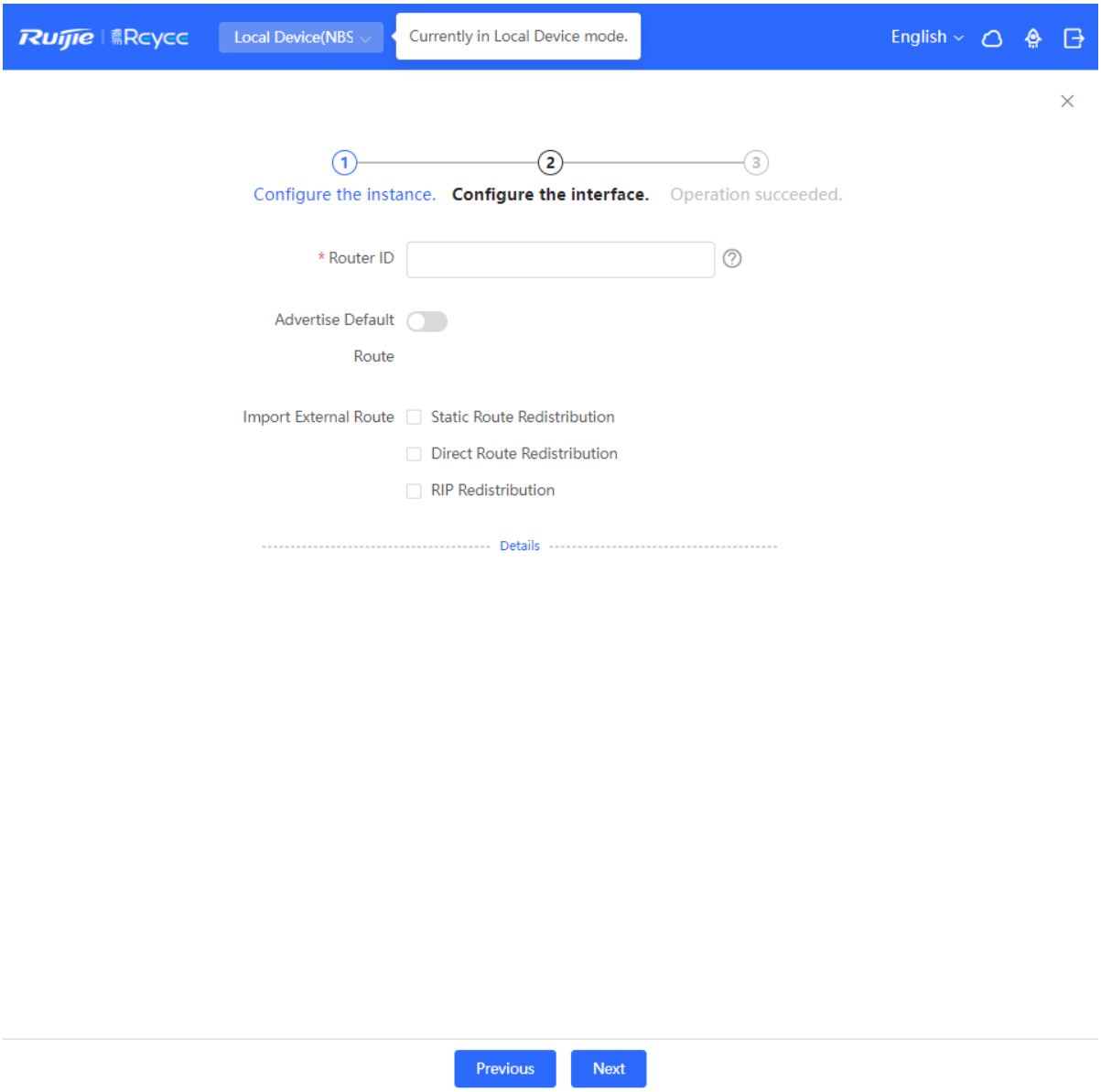
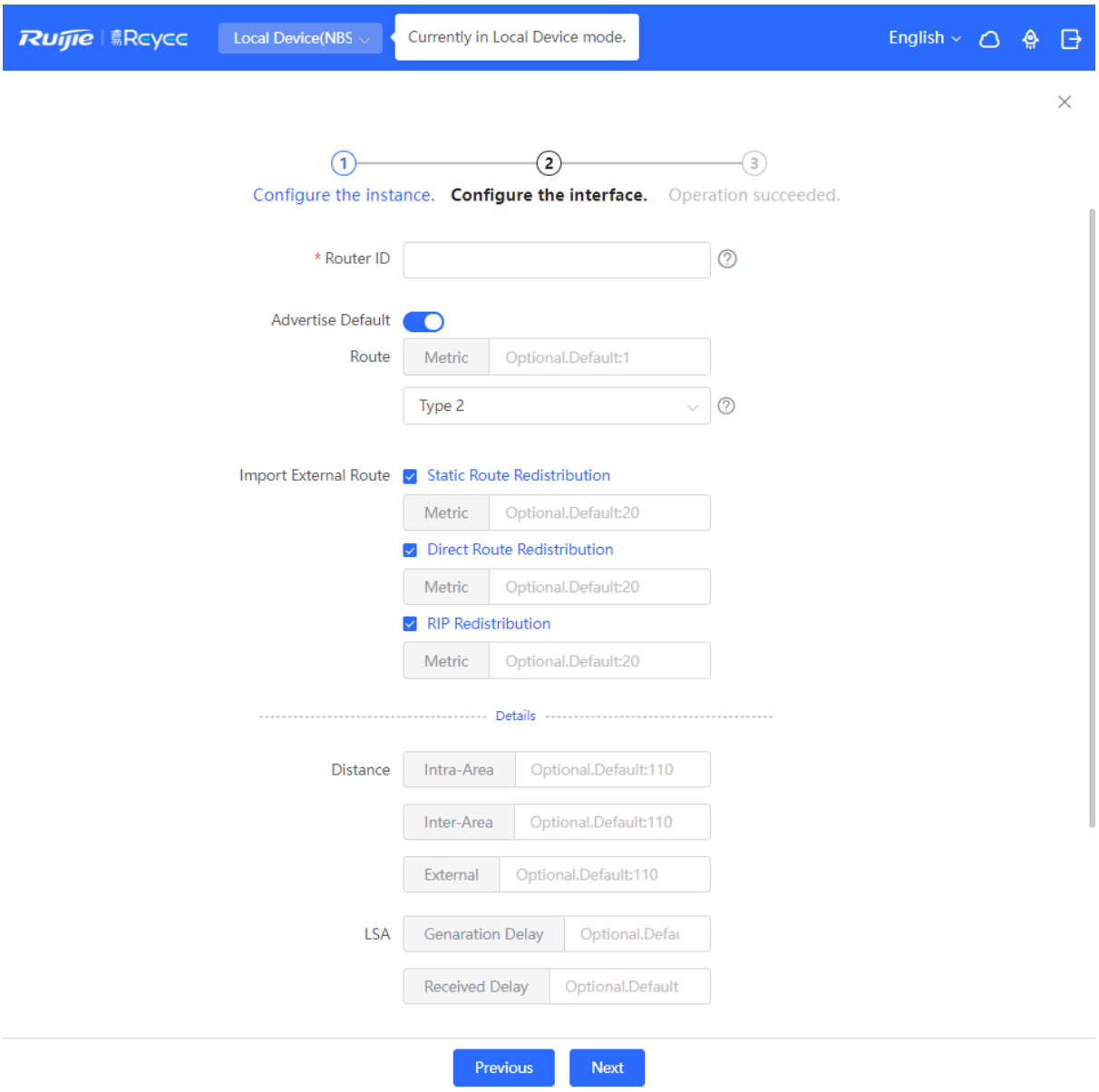


Table 7-14 Instance Configuration Parameters

Parameter	Description
Instance ID	Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices.
Router ID	It identifies a router in an OSPF domain.

Parameter	Description
	Caution Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures.
Advertise Default Route	Generate a default route and send it to the neighbor. After this function is enabled, you need to enter the metric and select a type. The default metric is **1**. Type 1: The metrics displayed on different routers vary. Type 2: The metrics displayed on all routers are the same.
Import External Route	Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains. If **Static Route Redistribution** is selected, enter the metric, which is **20** by default. If **Direct Route Redistribution** is selected, enter the metric, which is **20** by default. If **RIP Redistribution** is selected, enter the metric, which is **20** by default.
Details	Expand the detailed configuration.


Ruijie | Rcycc
Local Device(NBS
Currently in Local Device mode.
English
1
2
3
Configure the instance.
Configure the interface.
Operation succeeded.
* Router ID
Advertise Default Route
Metric
Optional.Default:1
Type 2
Import External Route
Static Route Redistribution
Metric
Optional.Default:20
Direct Route Redistribution
Metric
Optional.Default:20
RIP Redistribution
Metric
Optional.Default:20
Details
Distance
Intra-Area
Optional.Default:110
Inter-Area
Optional.Default:110
External
Optional.Default:110
LSA
Genaration Delay
Optional.Defa
Received Delay
Optional.Default
Previous
Next

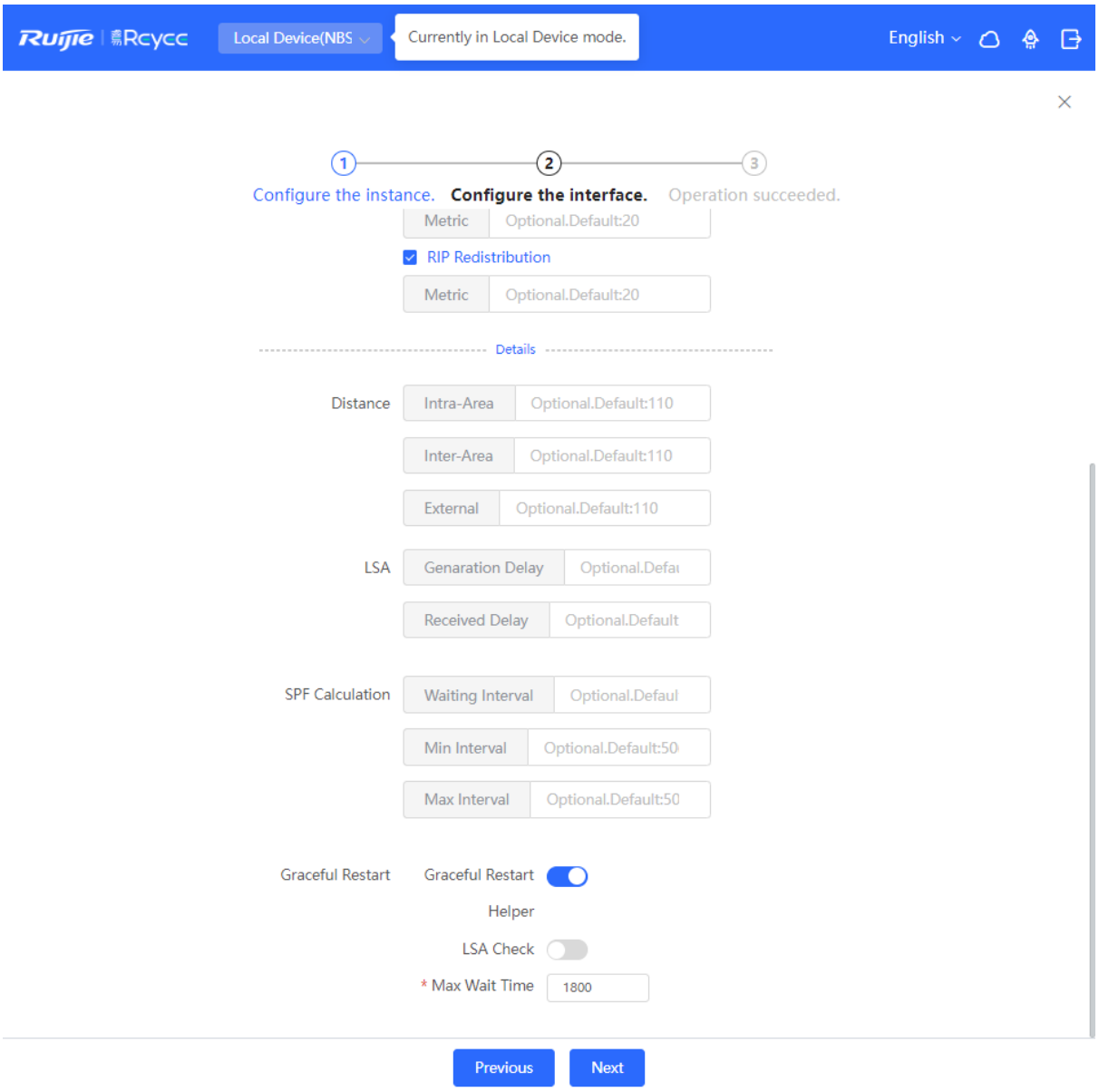


Table 7-15 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all **110**.
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.

Parameter	Description
SPF Calculation	When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources **Waiting Interval**: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. **Min Interval**: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. **Max Interval**: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.
Graceful Restart	Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services. **Graceful Restart Helper**: The Graceful Restart Helper function is enabled when this switch is turned on. **LSA Check**: LSA packets outside the domain are checked when this switch is turned on. **Max Wait Time**: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within **Max Wait Time**, the device exits the GR Helper mode. The default value is 1800 seconds.

2. Configure an interface.

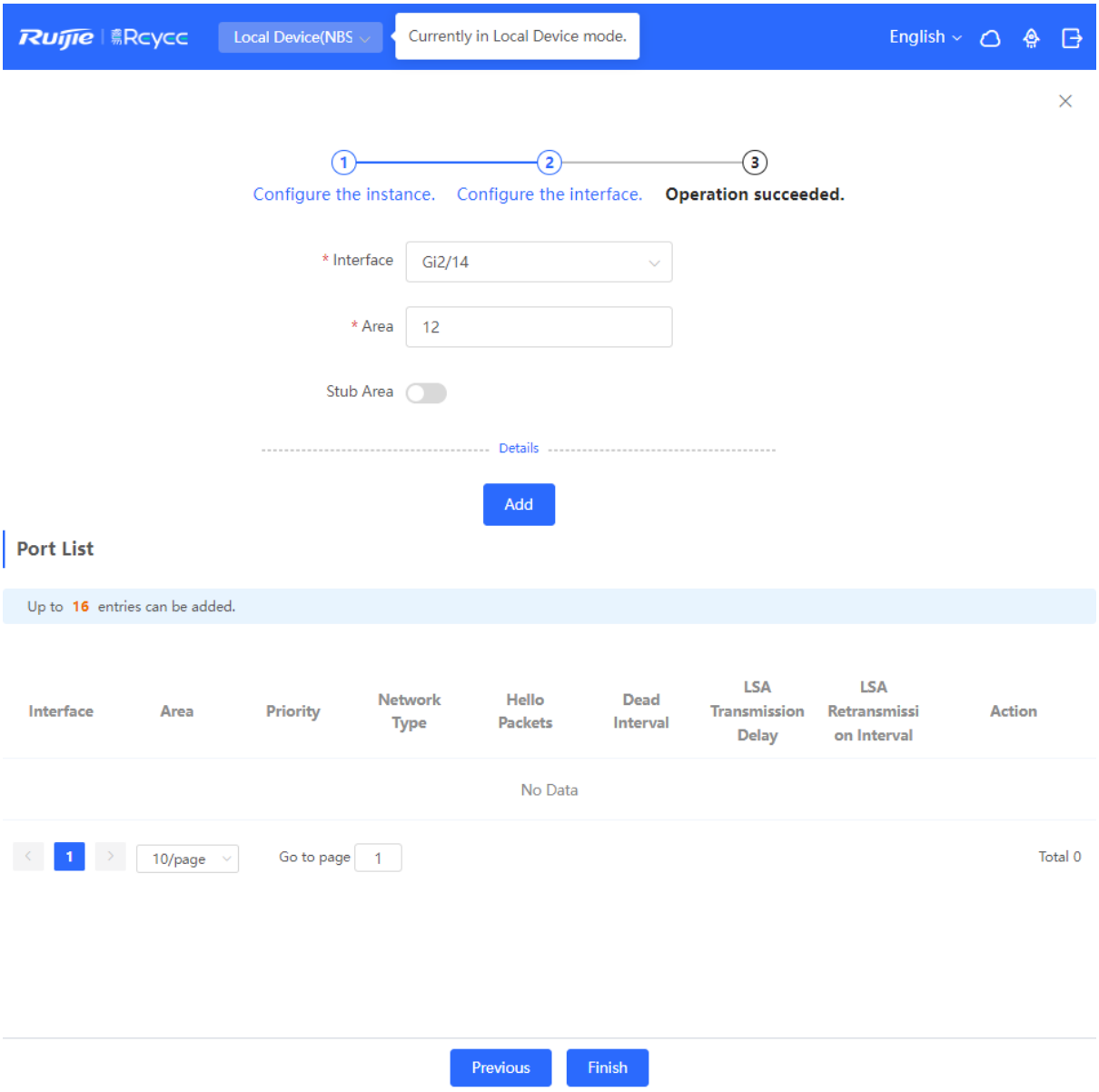
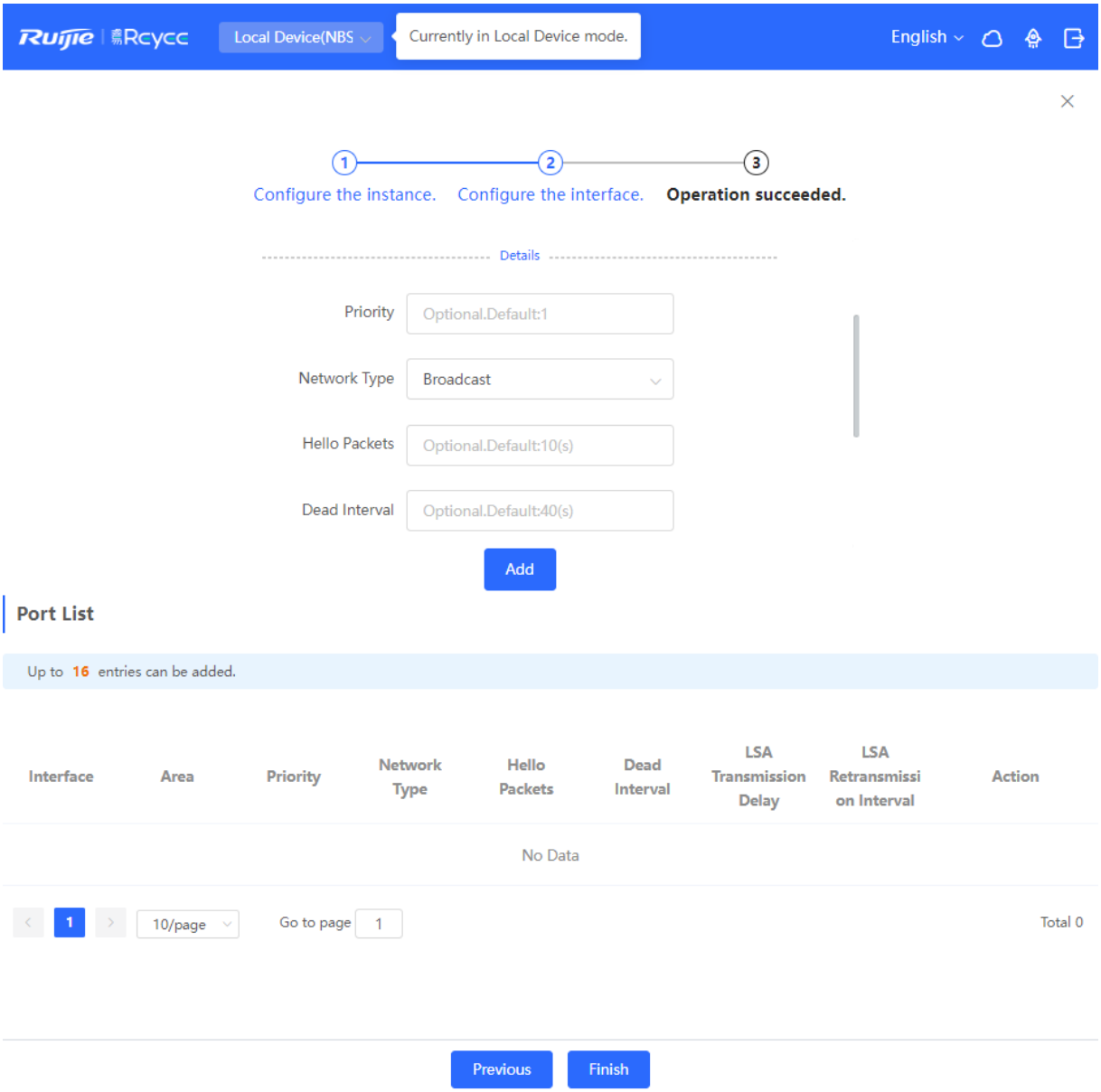
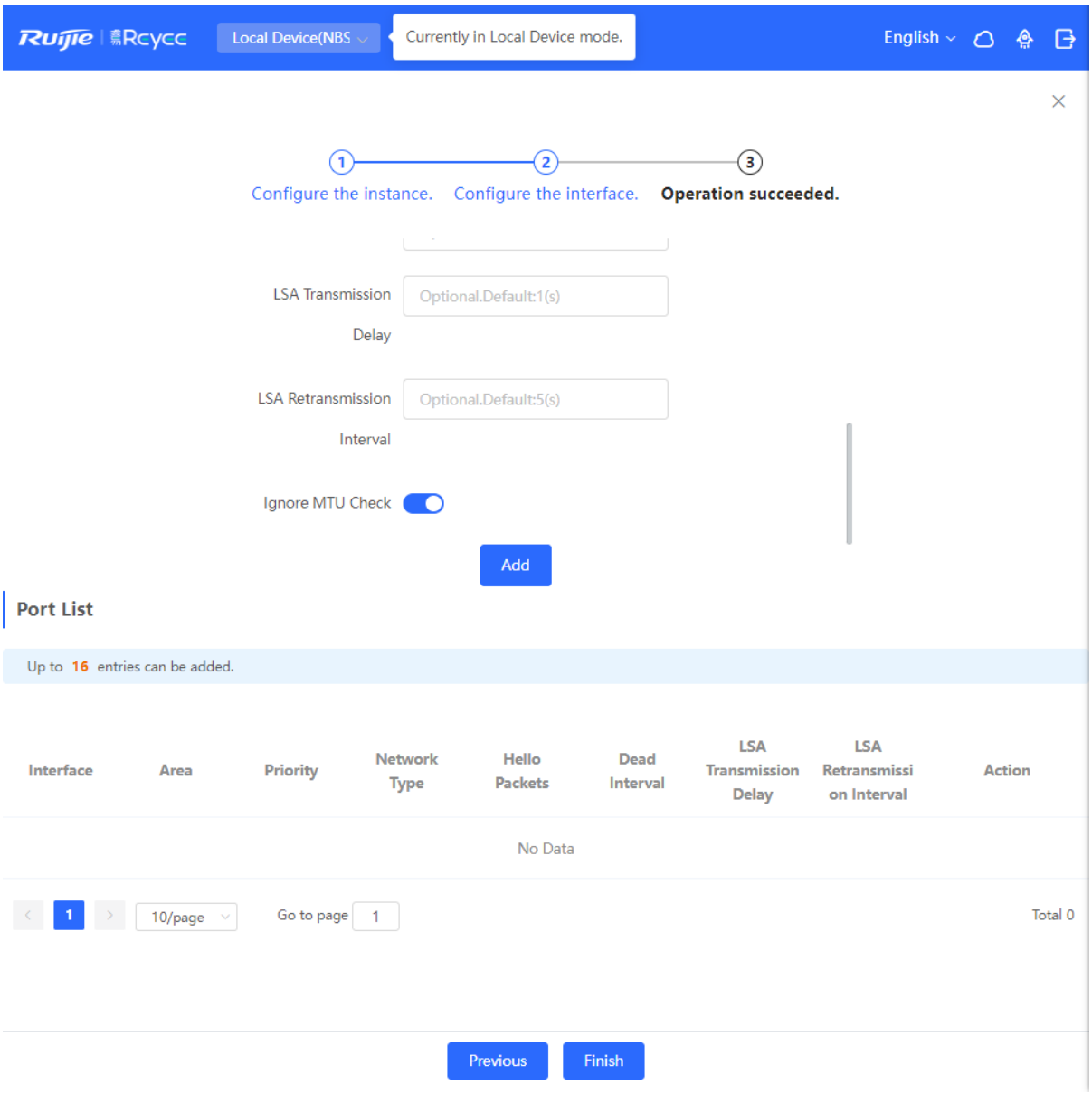


Table 7-16 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295
Stub Area	If **Stub Area** is enabled, you need to configure the area type and inter-area route isolation. Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing

Parameter	Description
	table in the area is small. Not-So-Stubby Area (NSSA): A few external routes can be imported.
Details	Expand the detailed configuration.




Local Device(NBS
Currently in Local Device mode.
English
Configure the instance.
Configure the interface.
Operation succeeded.
LSA Transmission Delay
Optional.Default:1(s)
LSA Retransmission Interval
Optional.Default:5(s)
Ignore MTU Check
Add
Port List
Up to 16 entries can be added.
Interface
Area
Priority
Network Type
Hello Packets
Dead Interval
LSA Transmission Delay
LSA Retransmission Interval
Action
No Data
1
10/page
Go to page
1
Total 0
Previous
Finish

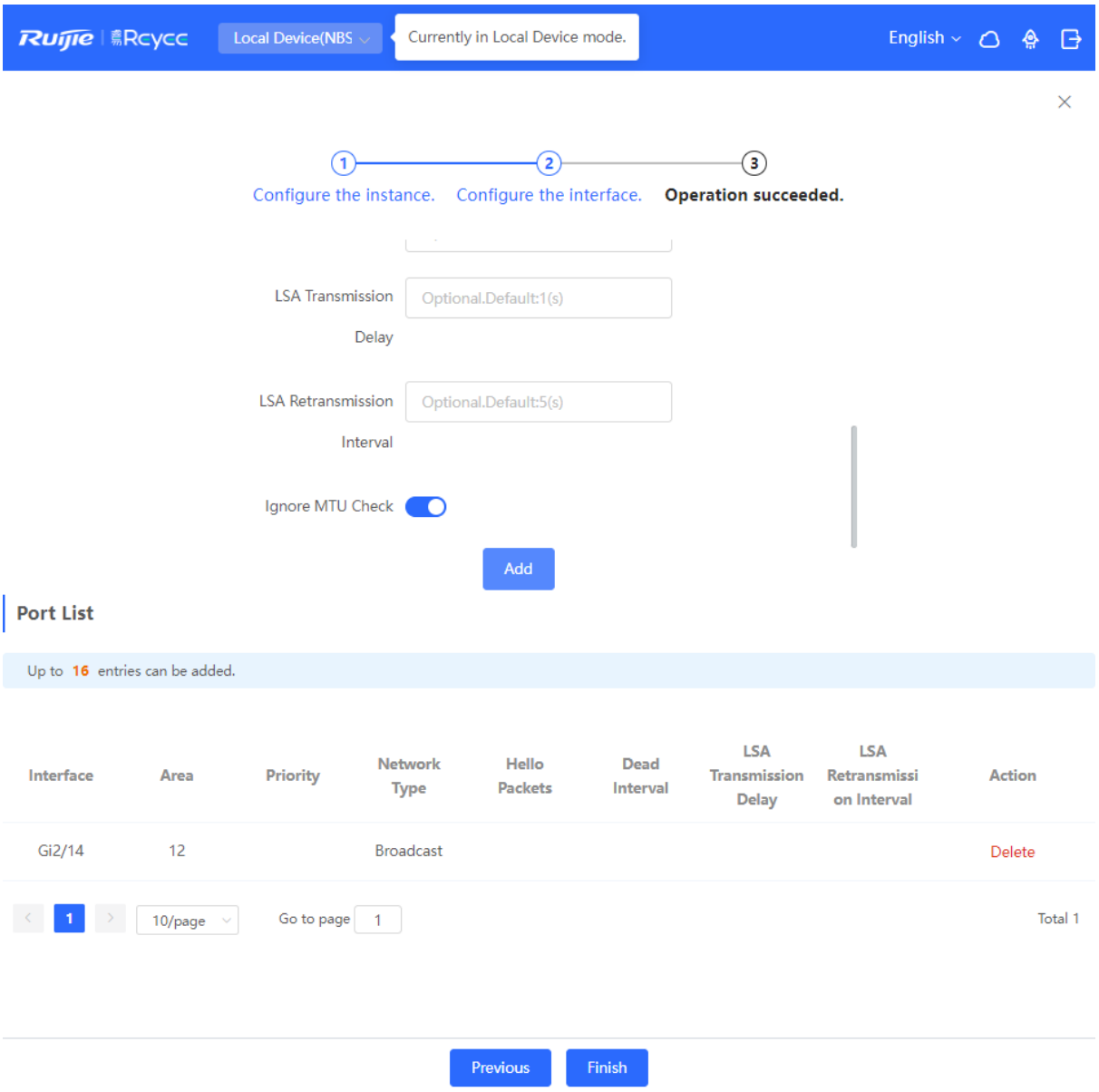
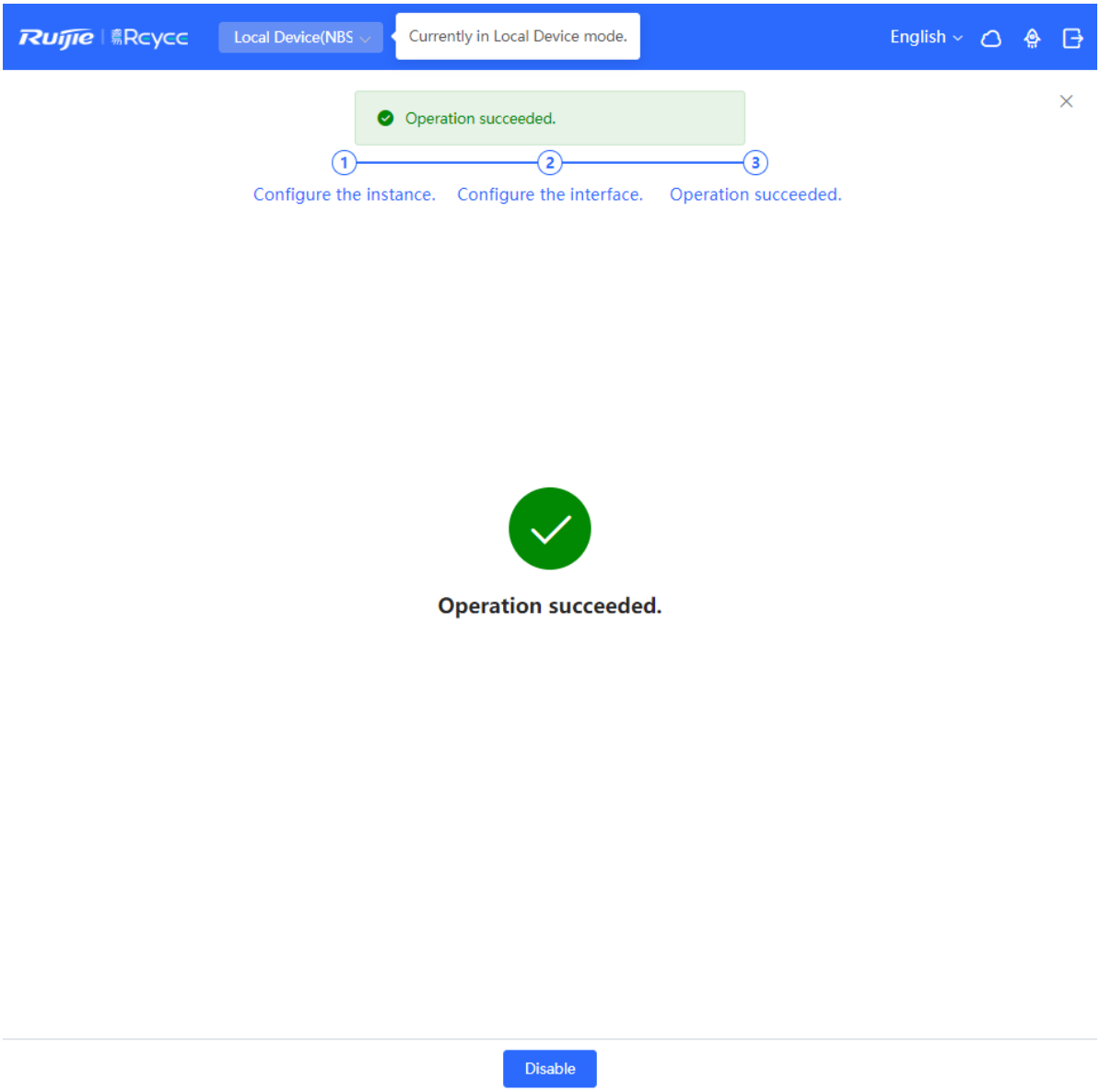


Table 7-17 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
Network Type	Broadcast Unicast Multicast Non-Broadcast Multiple Access

Parameter	Description
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	**No Auth**: The protocol packets are not authenticated. It is the default value. **Plain Text**: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. **MD5**: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

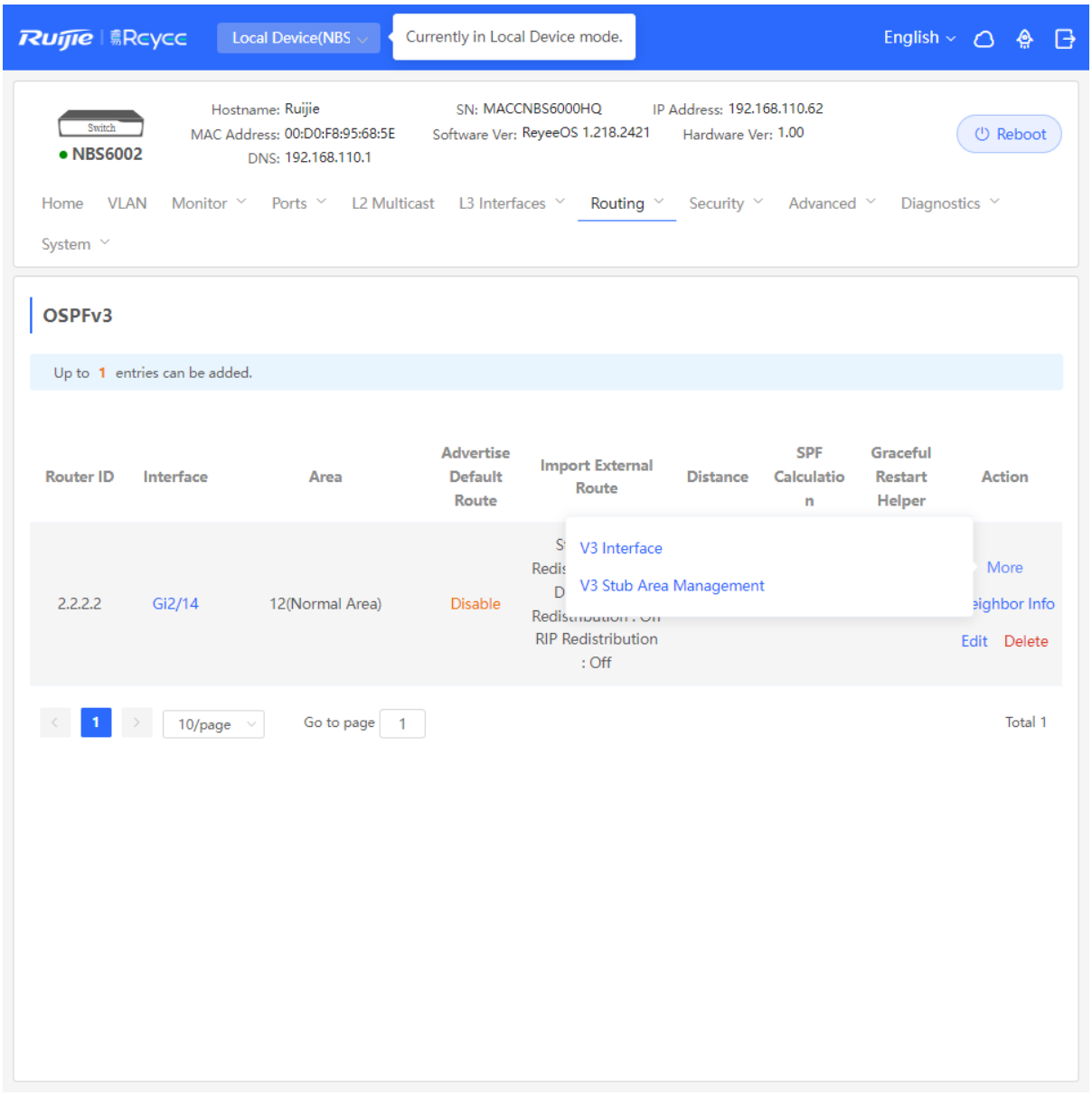
3. Complete the configuration.

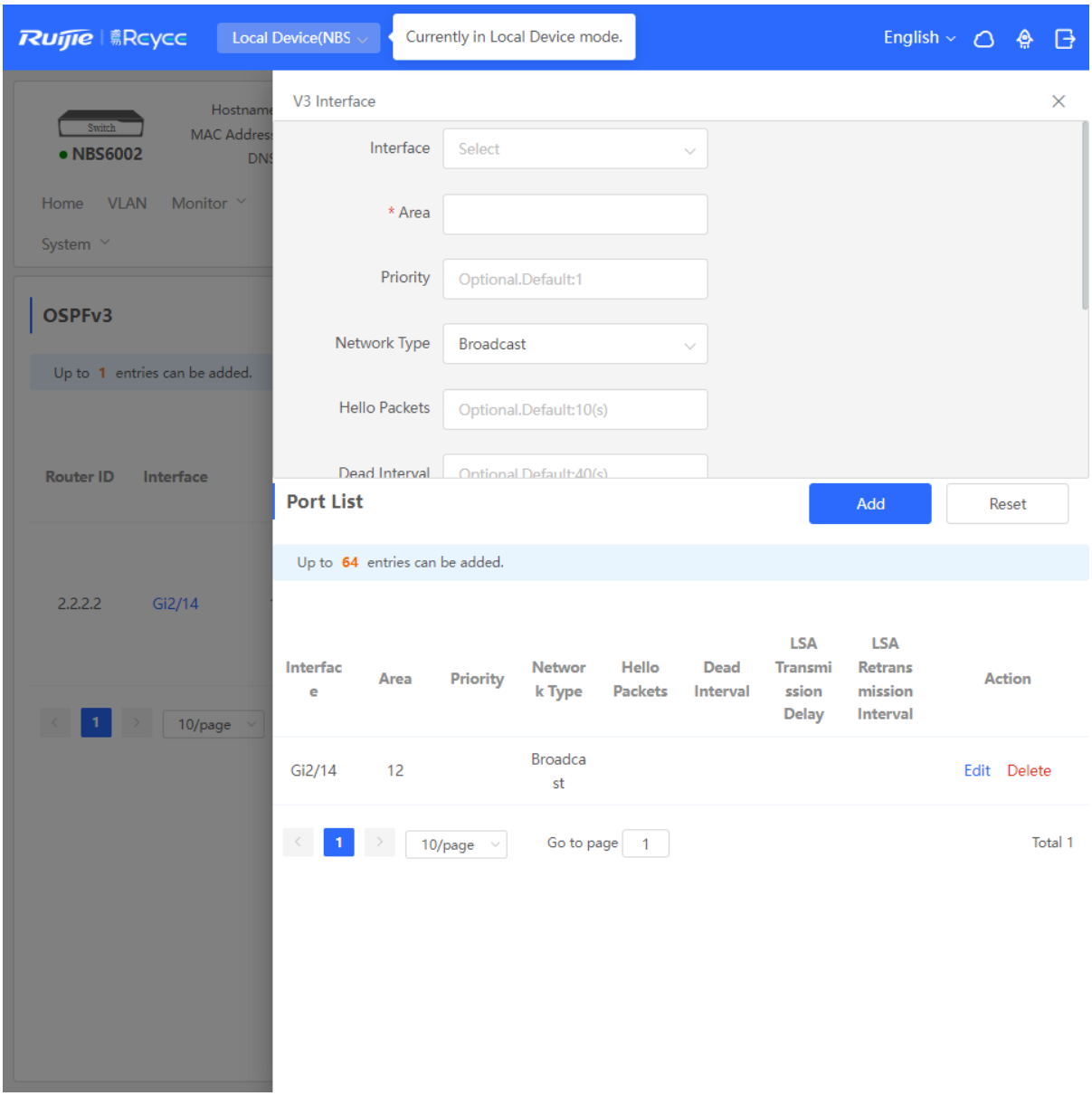


After completing the configuration, you can choose **Local Device** > **Routing** > **OSPFv3** and view the instance list.

7.6.2 Adding an OSPFv3 Interface

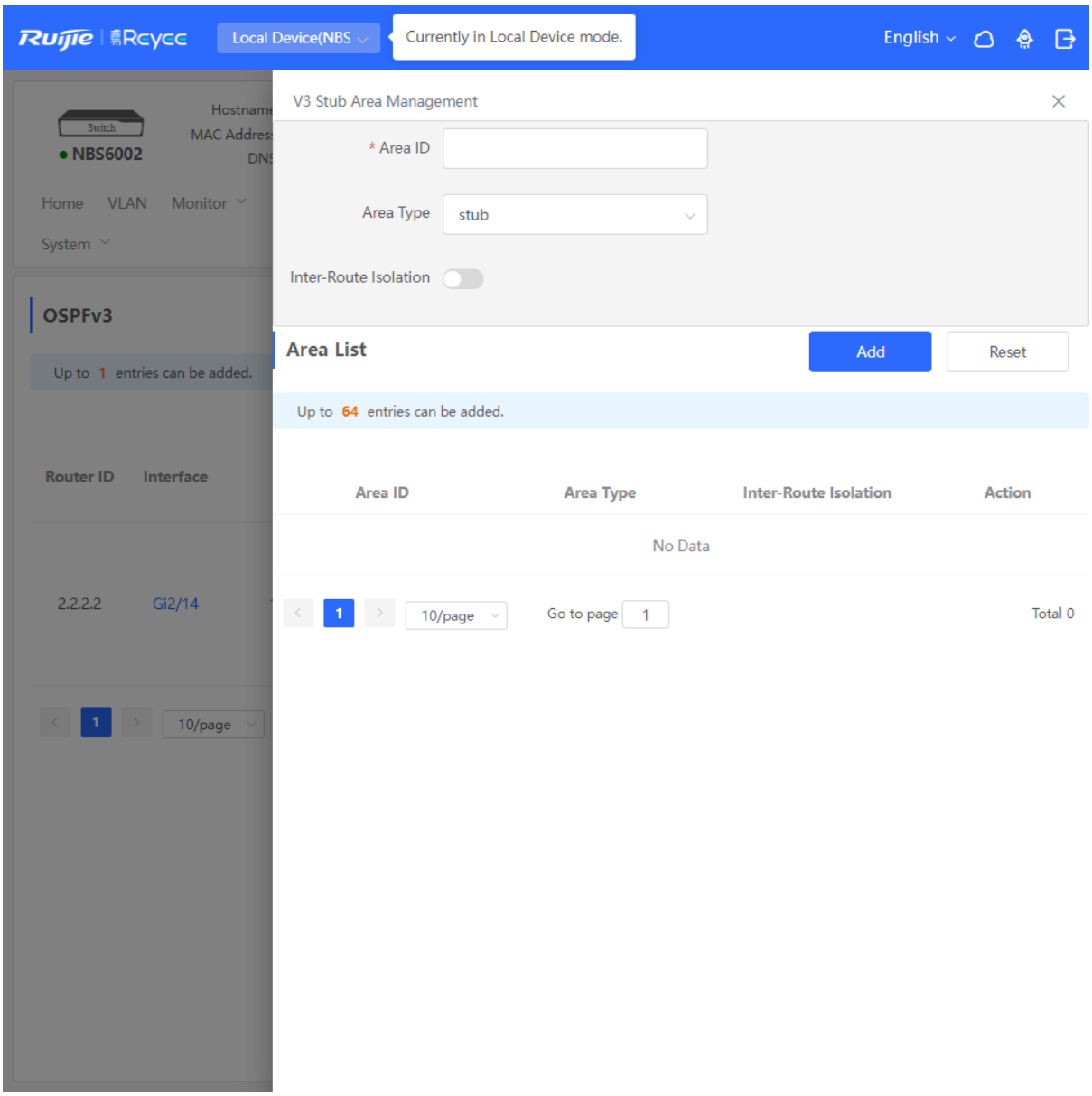
Choose **Local Device** > **Routing** > **OSPFv3**, click **More** in the **Action** column, and select **V3 Interface**.


Local Device(NBS
Currently in Local Device mode.
English
Switch
NBS6002
Hostname: Ruijie
MAC Address: 00:D0:F8:95:68:5E
DNS: 192.168.110.1
SN: MACCNBS6000HQ
Software Ver: ReyeeOS 1.218.2421
IP Address: 192.168.110.62
Hardware Ver: 1.00
Reboot
Home
VLAN
Monitor
Ports
L2 Multicast
L3 Interfaces
Routing
Security
Advanced
Diagnostics
System
OSPFv3
Up to 1 entries can be added.
Router ID
Interface
Area
Advertise Default Route
Import External Route
Distance
SPF Calculation
Graceful Restart Helper
Action
V3 Interface
V3 Stub Area Management
2.2.2.2
Gi2/14
12(Normal Area)
Disable
RIP Redistribution : Off
More
Edit
Delete
10/page
Go to page
1
Total 1



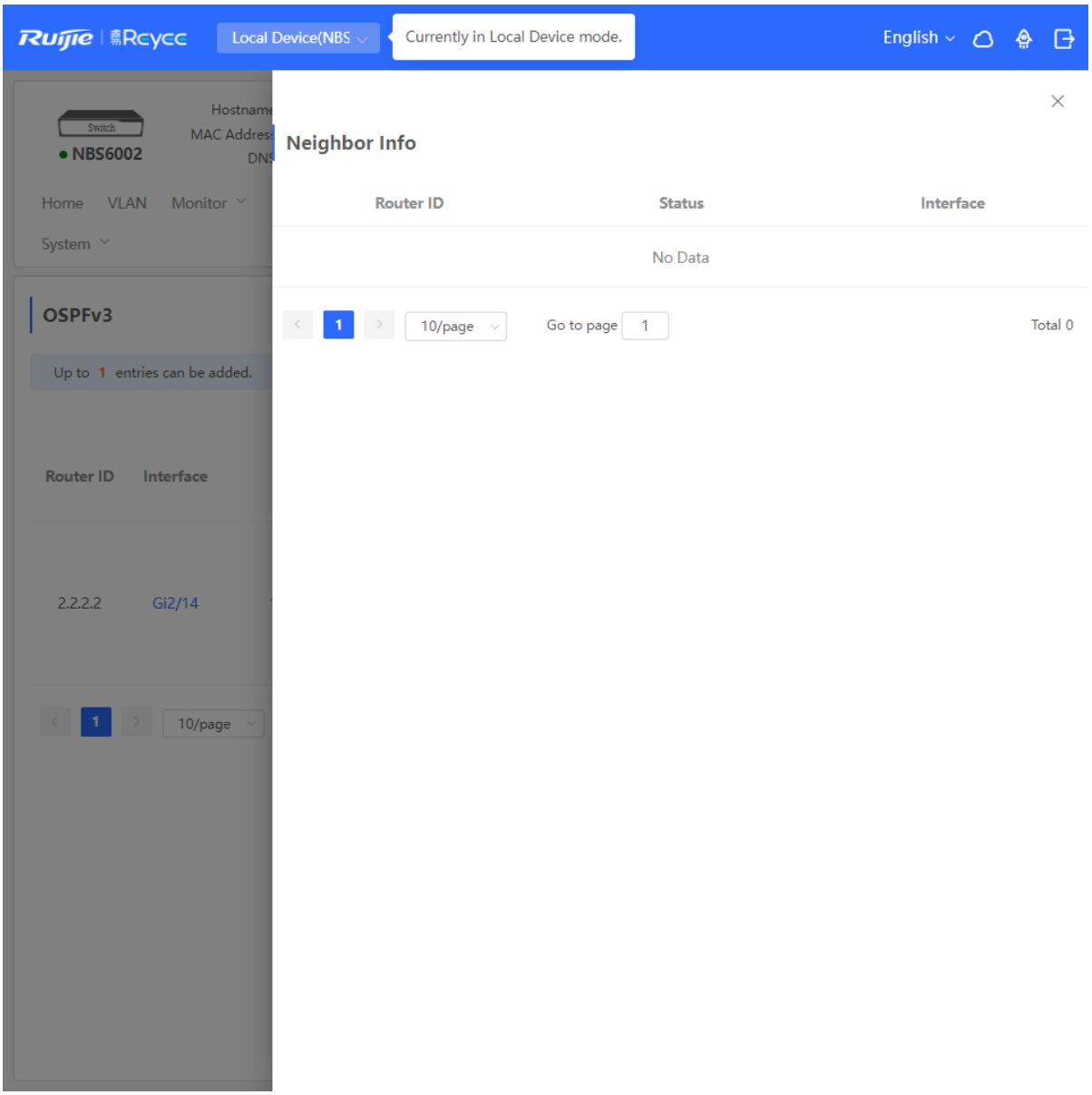
7.6.3 Managing OSPFv3 Stub Areas

Choose **Local Device** > **Routing** > **OSPFv3**, click **More** in the **Action** column, and select **V3 Stub Area Management**.

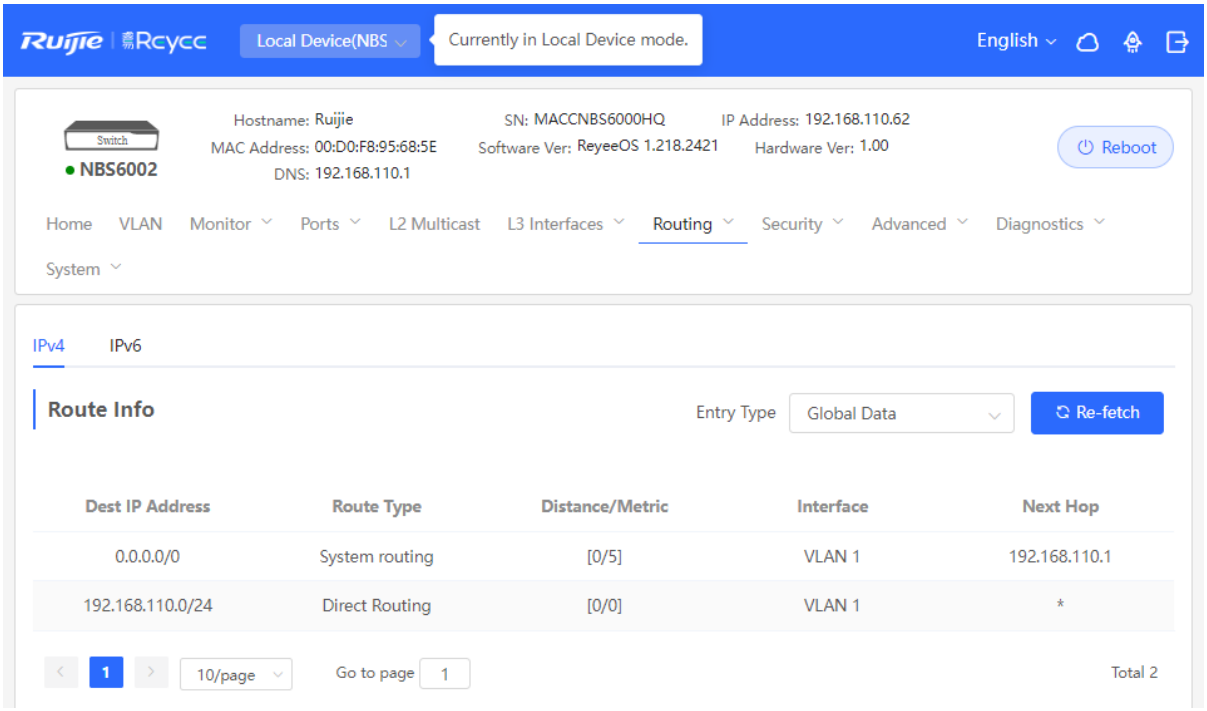


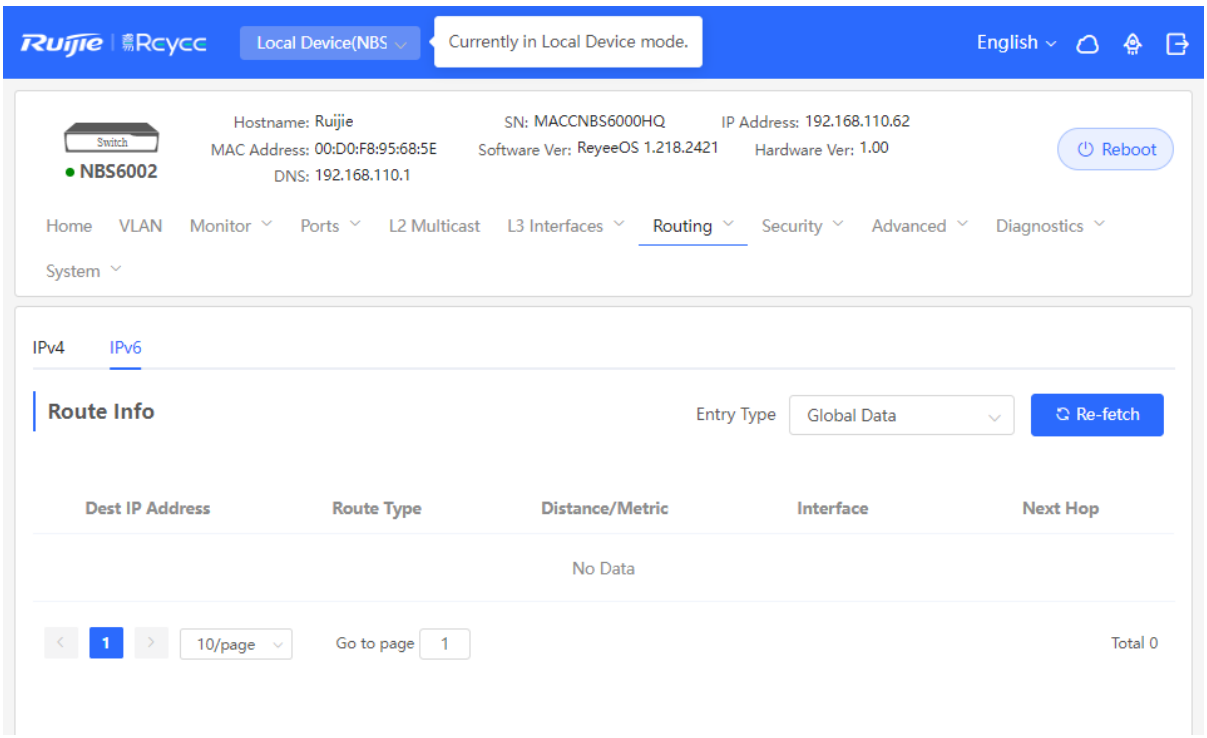
7.6.4 Viewing OSPFv3 Neighbor Information

Choose **Local Device** > **Routing** > **OSPFv3**, and click **Neighbor Info** in the **Action** column.


Local Device(NBS
Currently in Local Device mode.
English
NBS6002
Home
VLAN
Monitor
System
OSPFv3
Up to 1 entries can be added.
Router ID
Interface
2.2.2.2
Gi2/14
1
10/page
Neighbor Info
Router ID
Status
Interface
No Data
1
10/page
Go to page 1
Total 0

7.7 Routing Table Info





8 Firewall Management

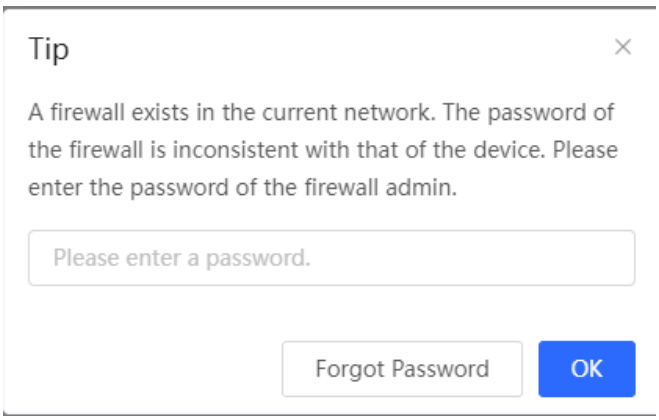
After a firewall is added to the network, you can manage and configure the firewall on the Web management system.

8.1 Viewing Firewall Information

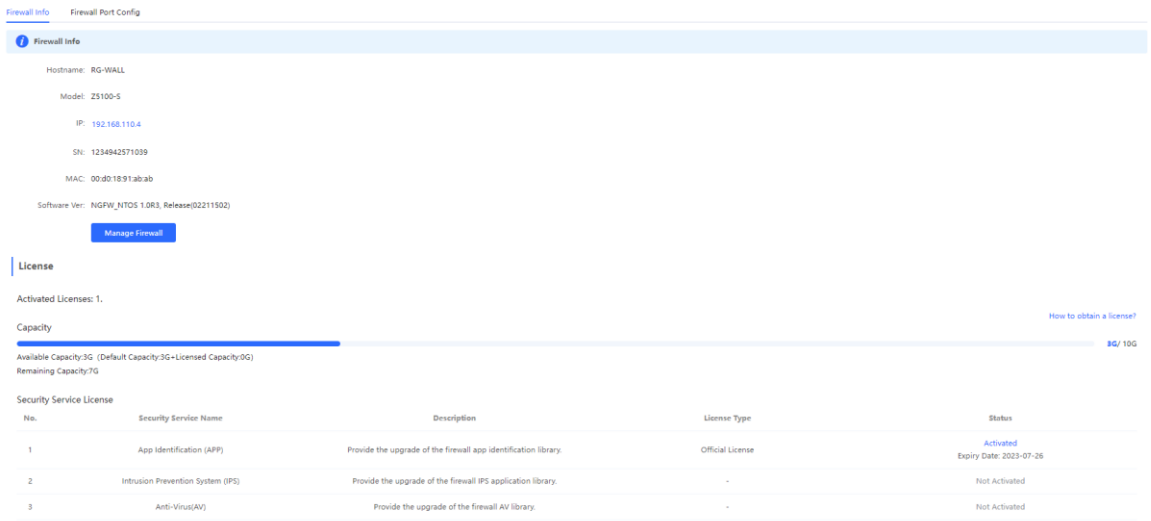
You can view the basic information and license of the firewall on the Web management system.

Choose **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**.



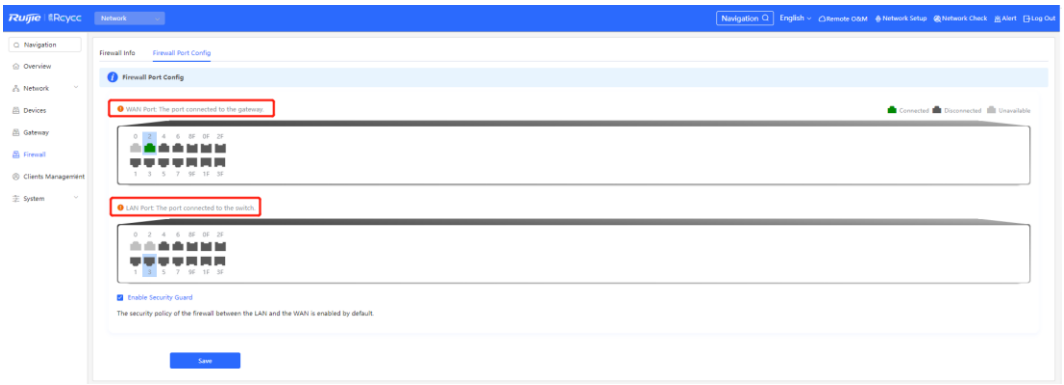
(2) The basic information, capacity, and security service license of the firewall are displayed on the Web management system.



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.

8.2 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**.



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

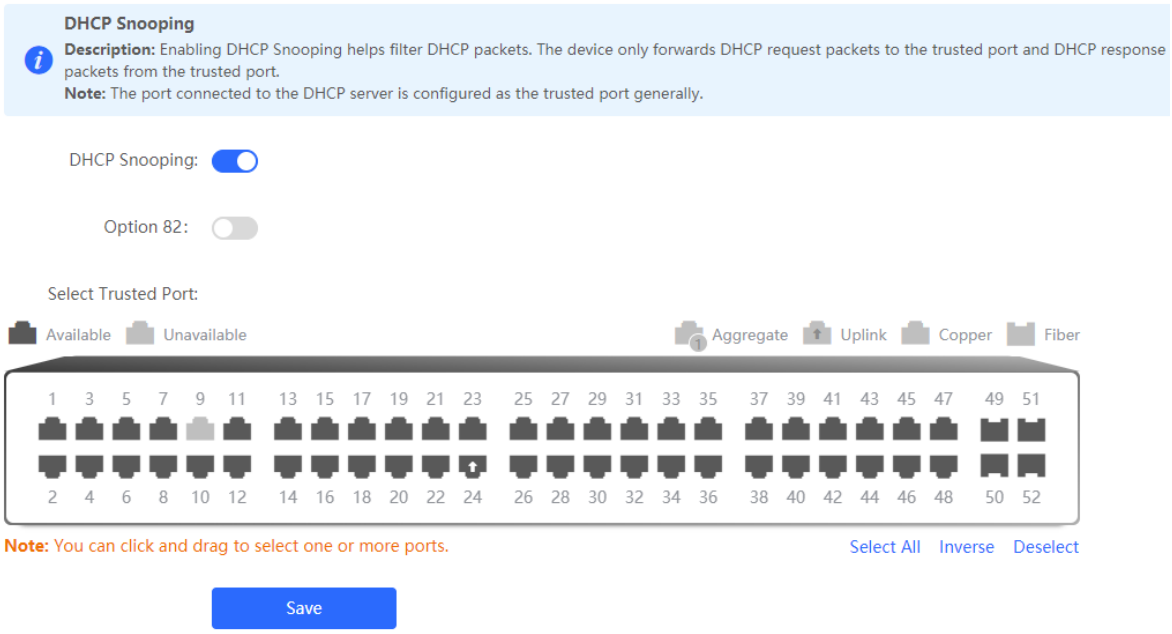
Choose **Local Device** > **Security** > **DHCP Snooping**.

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.

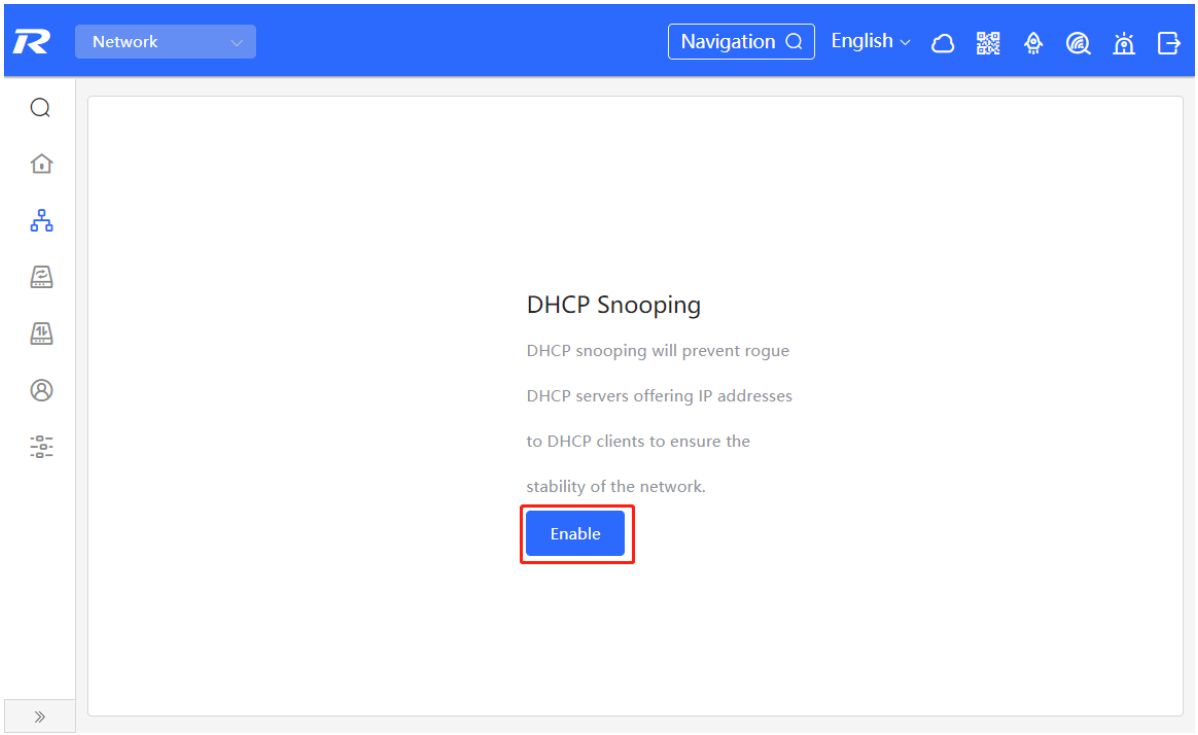


9.1.3 Batch Configuring Network Switches

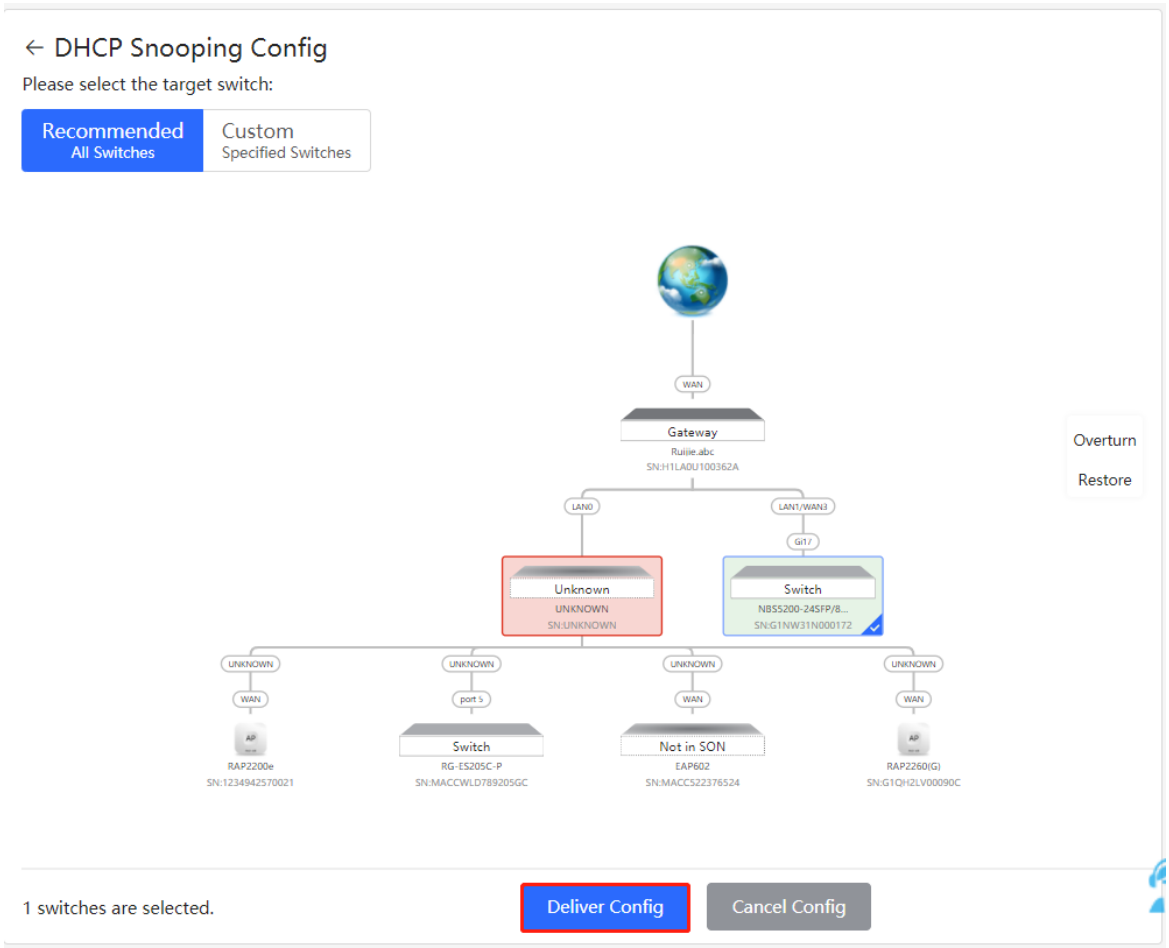
Choose **Network** > **DHCP Snooping**.

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 the occurrence of "the Internet terminal in the original network obtains the IP address assigned by the privately accessed router", to guarantee the stability of the network.

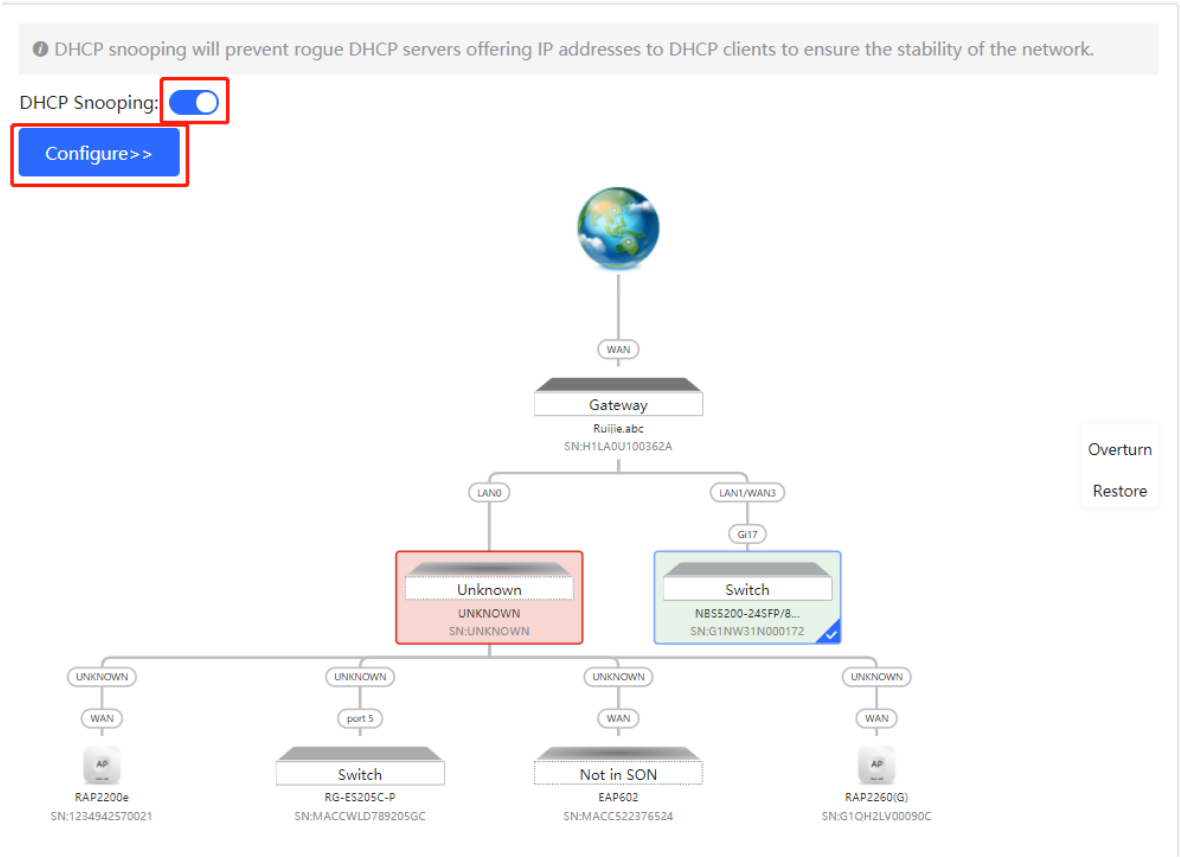
(1) Click **Enable** to access the **DHCP Snooping Config** page.



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



(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.



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.

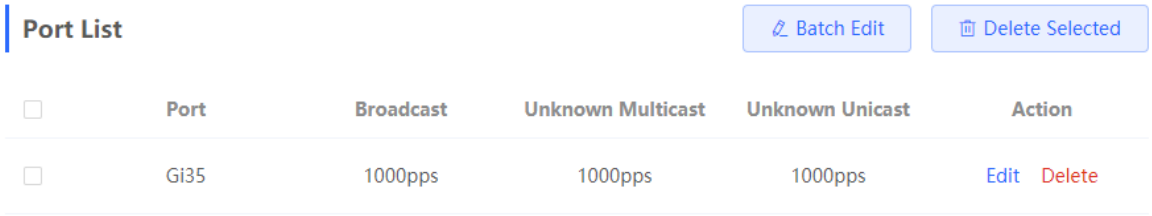
9.2.2 Procedure

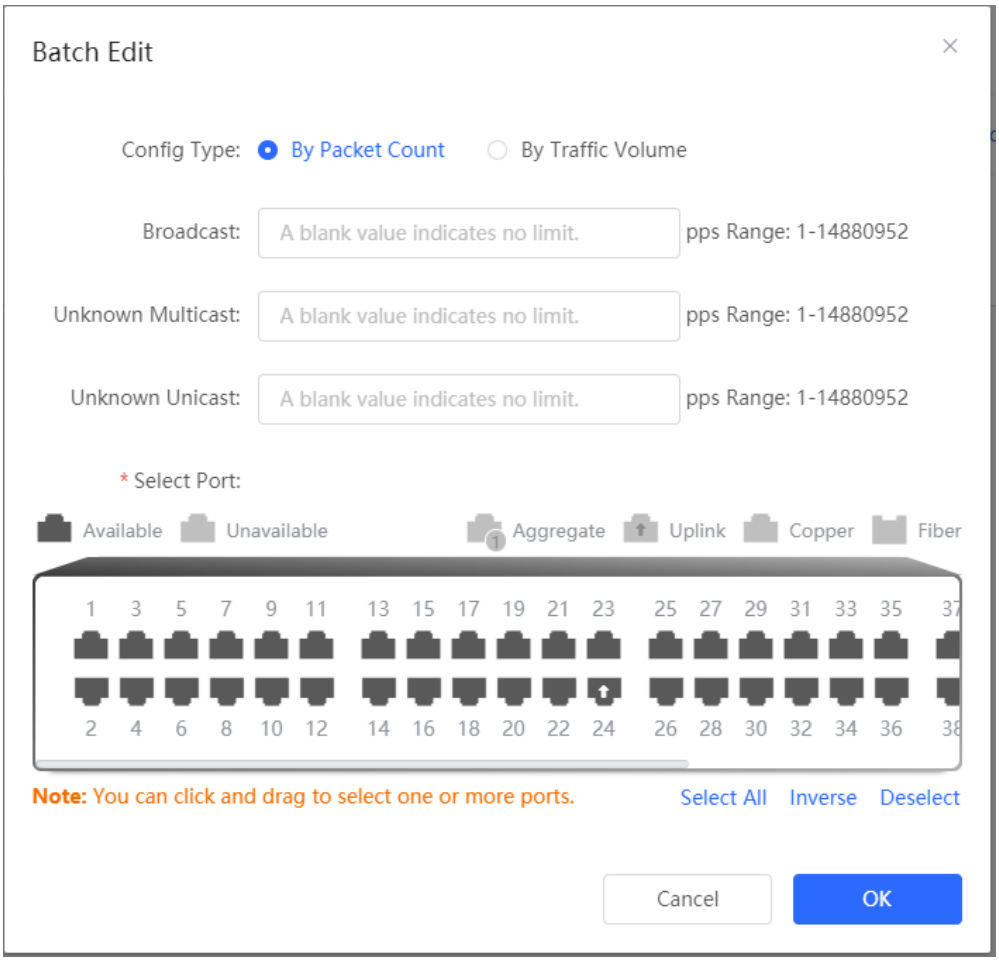
Choose **Local Device** > **Security** > **Storm Control**.

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.





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.

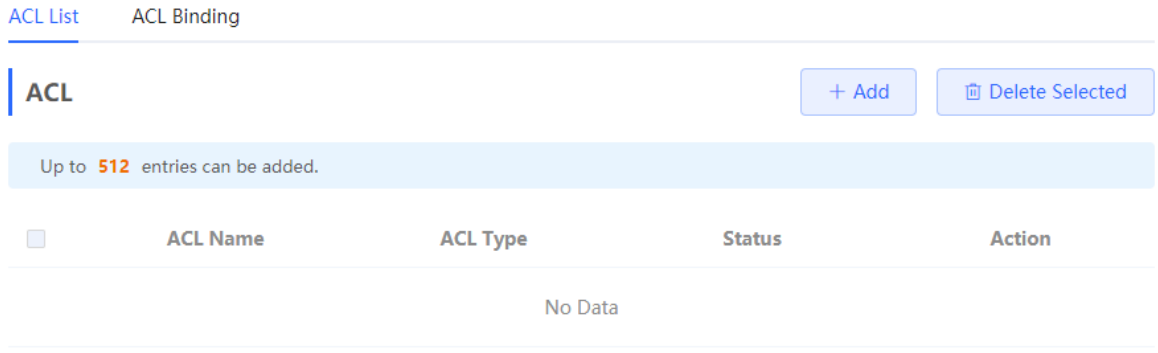
9.3.2 Creating ACL Rules

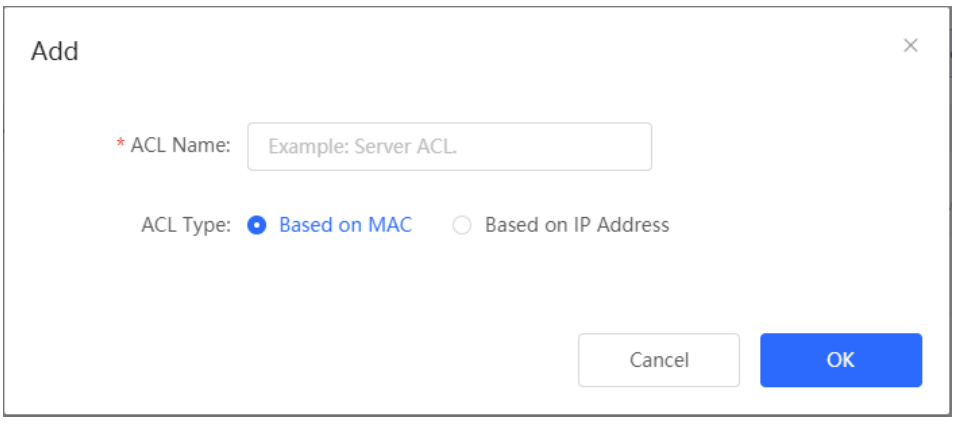
Choose **Local Device** > **Security** > **ACL** > **ACL List**.

(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.





(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.

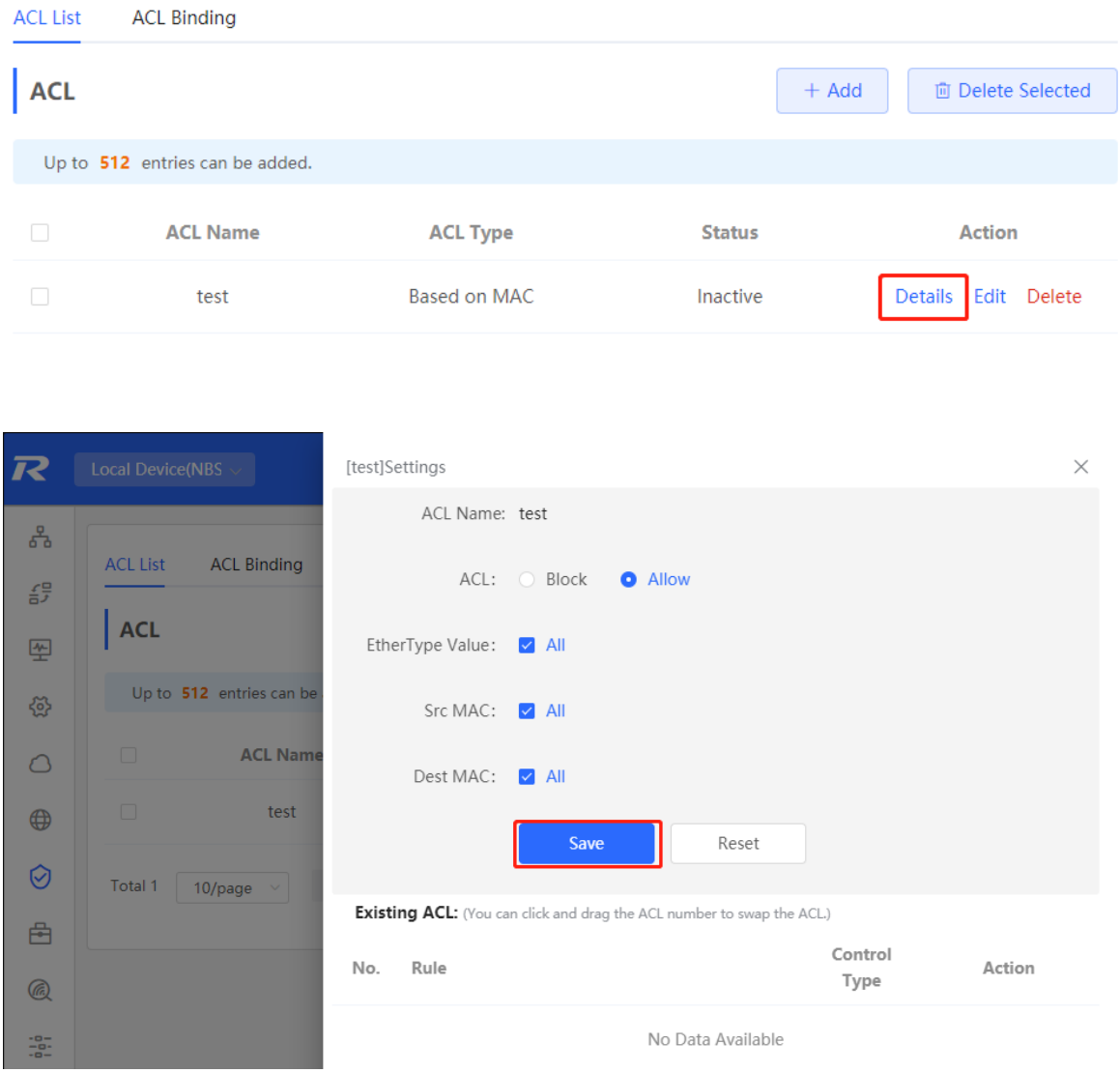


Table 9-1 Description of ACL Rule Configuration Parameters

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.

Parameter	Description
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.

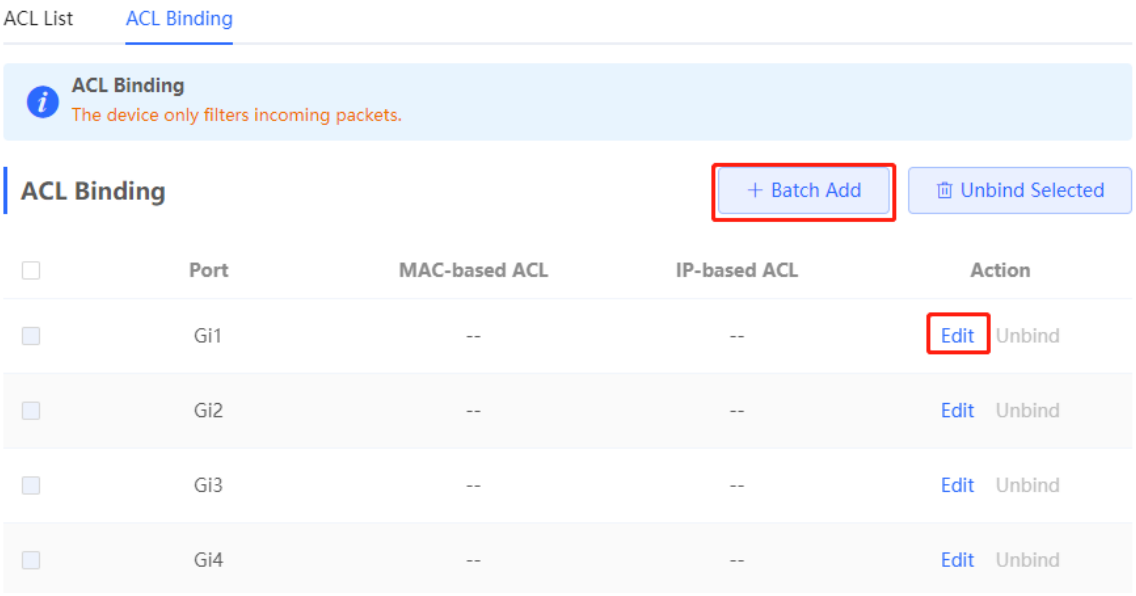
9.3.3 Applying ACL Rules

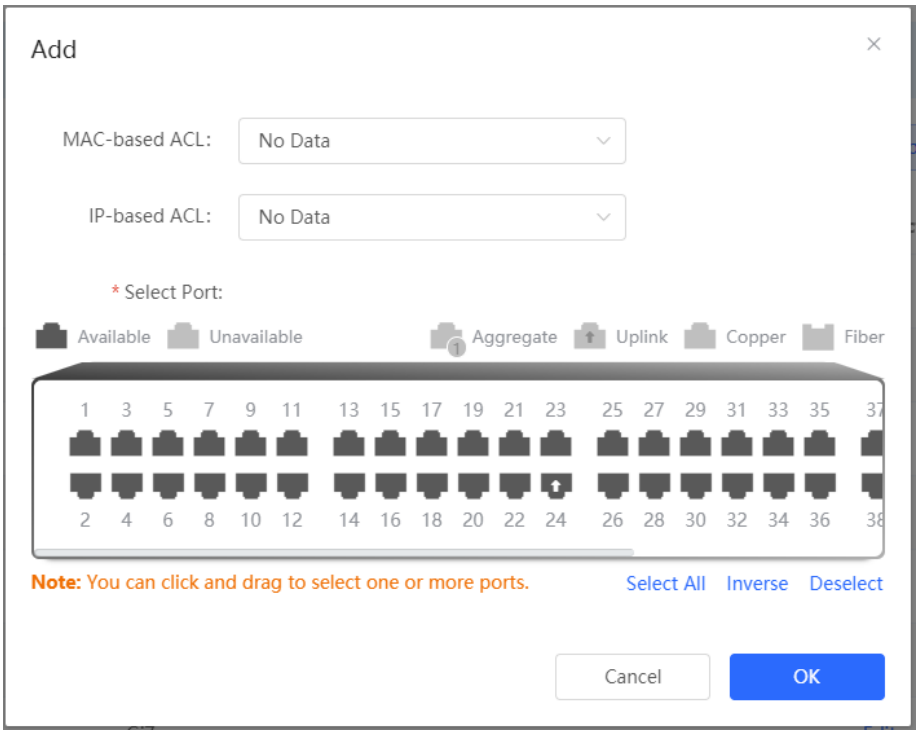
Choose **Local Device** > **Security** > **ACL** > **ACL List**.

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

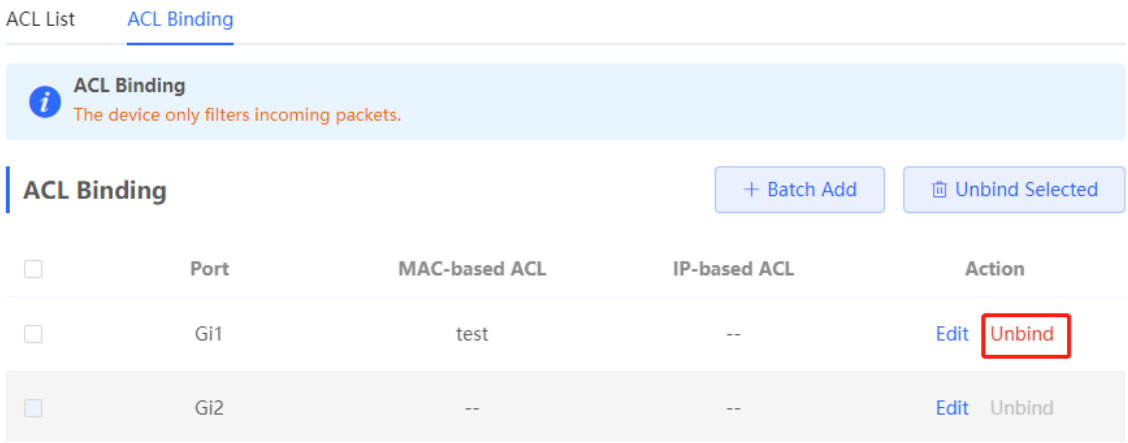
Note

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





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.

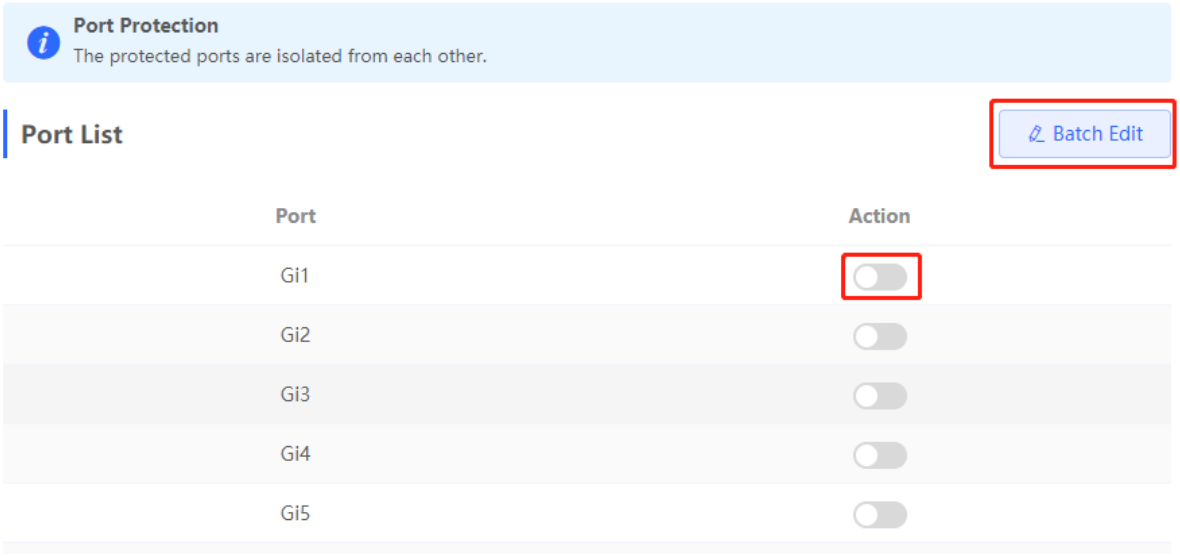


9.4 Port Protection

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.**



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

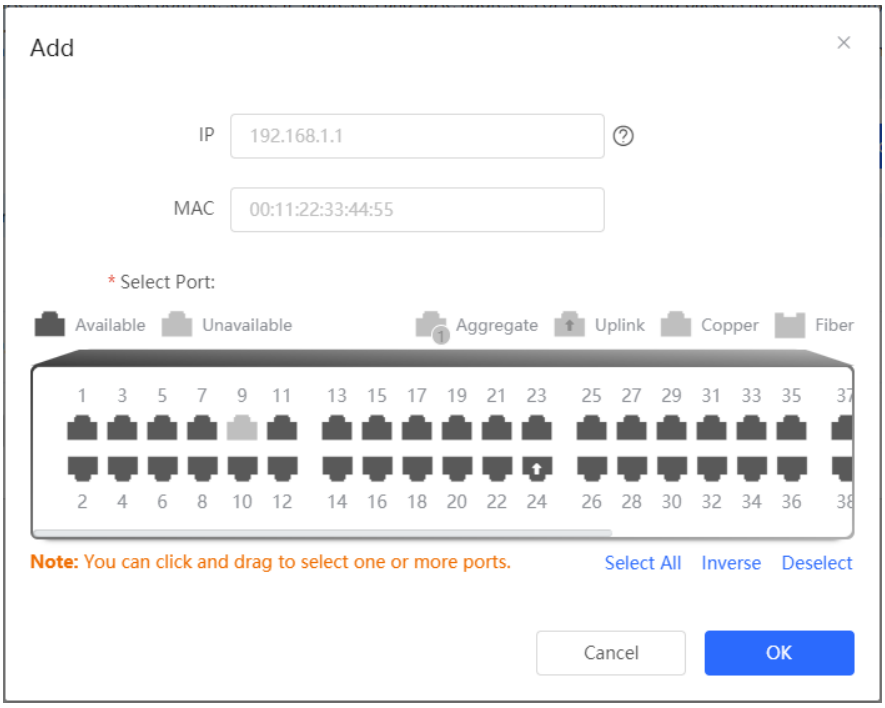
Choose **Local Device** > **Security** > **IP-MAC Binding**.

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.

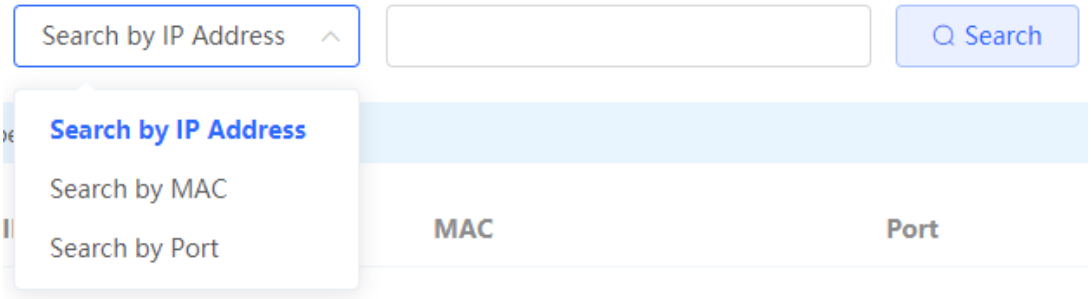
Caution

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.



2. Searching Binding Entries

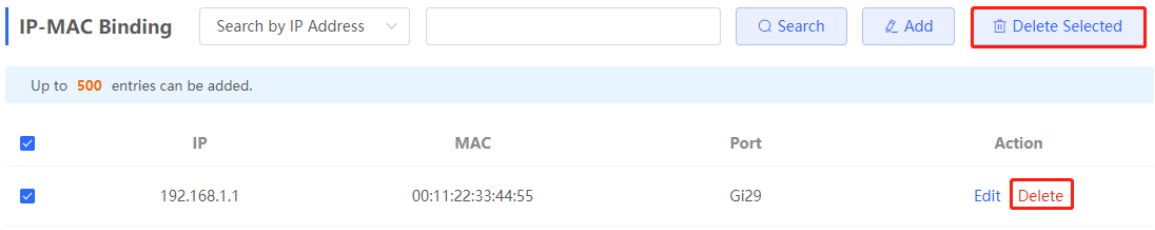
The search box in the upper-right corner supports finding binding entries based on IP addresses, MAC addresses or ports. Select the search type, enter the search string, and click **Search**. Entries that meet the search criteria are displayed in the list.



3. Deleting an IP-MAC Binding Entry

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

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



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

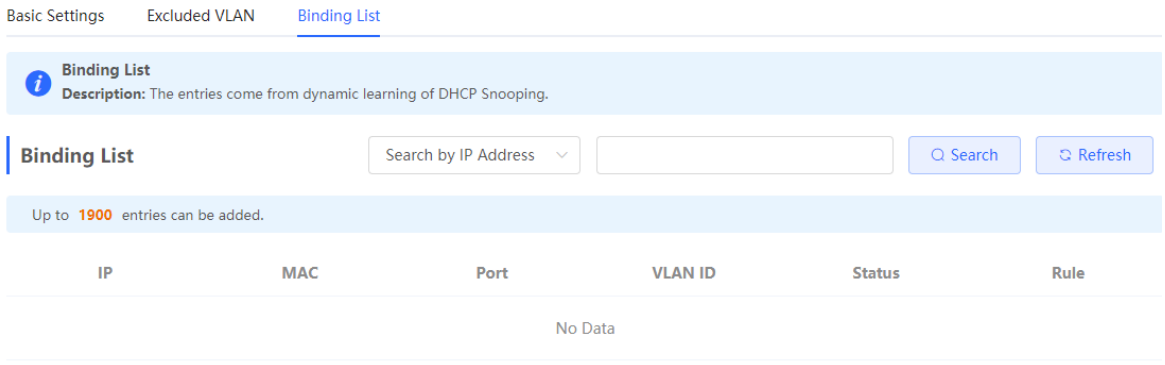
IP Source Guard should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see 7.1 for details.

9.6.2 Viewing Binding List

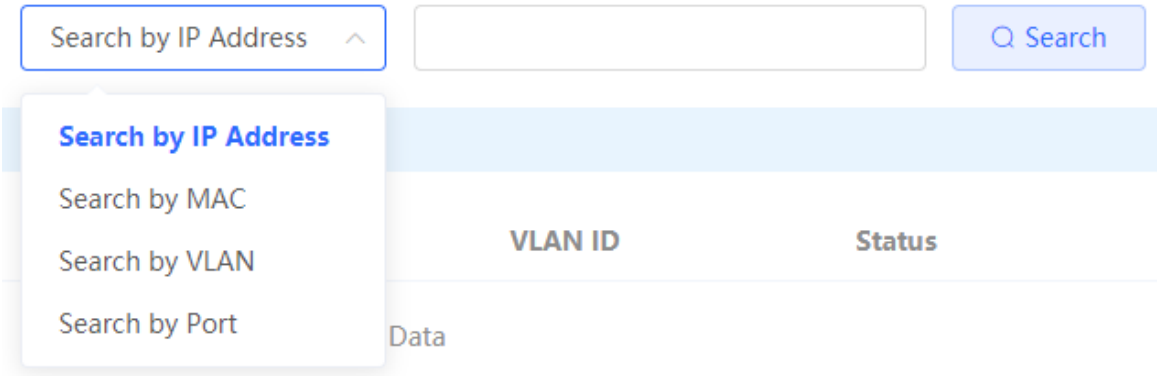
Choose **Local Device** > **Security** > **IP Source Guard** > **Binding List**.

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**.



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**.

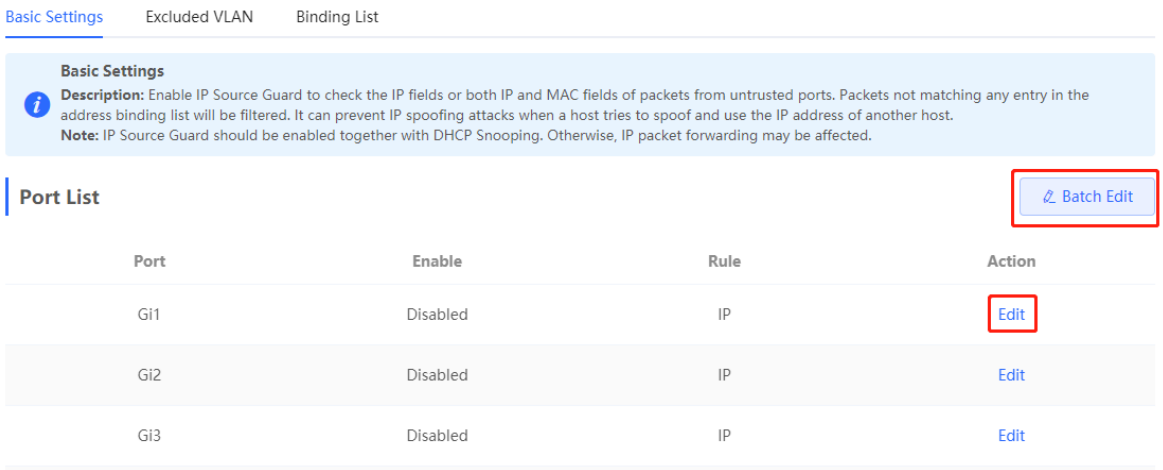
In Port List, click **Edit** in the **Action** column. Select **Enabled** and select the match rule, and click **OK**.

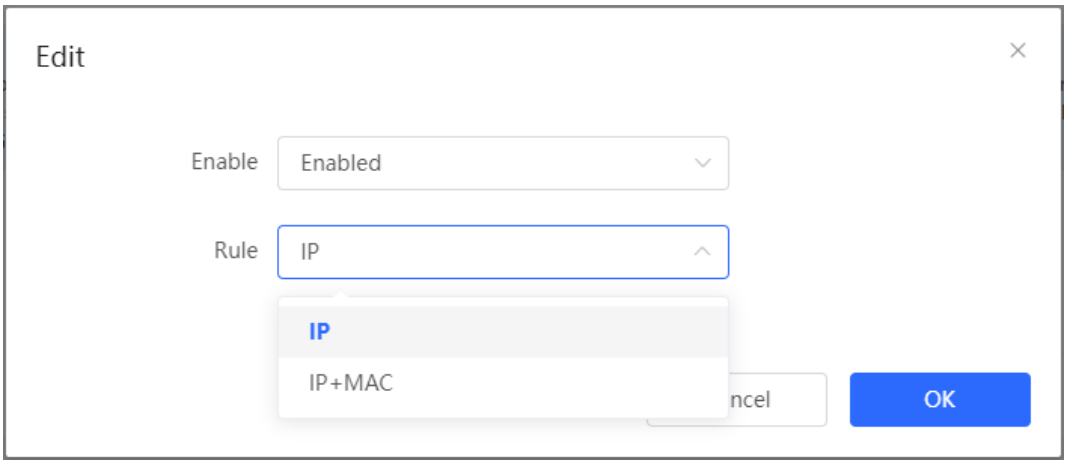
There are two match rules:

- 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.





9.6.4 Configuring Exceptional VLAN Addresses

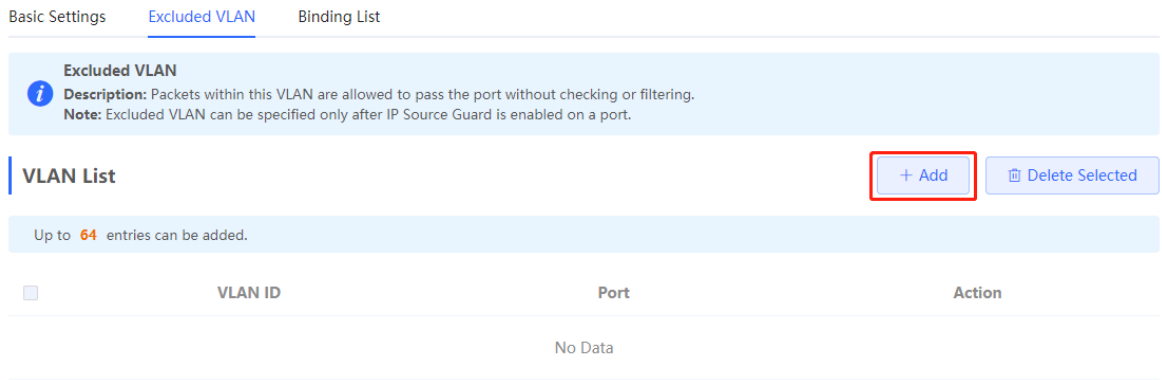
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

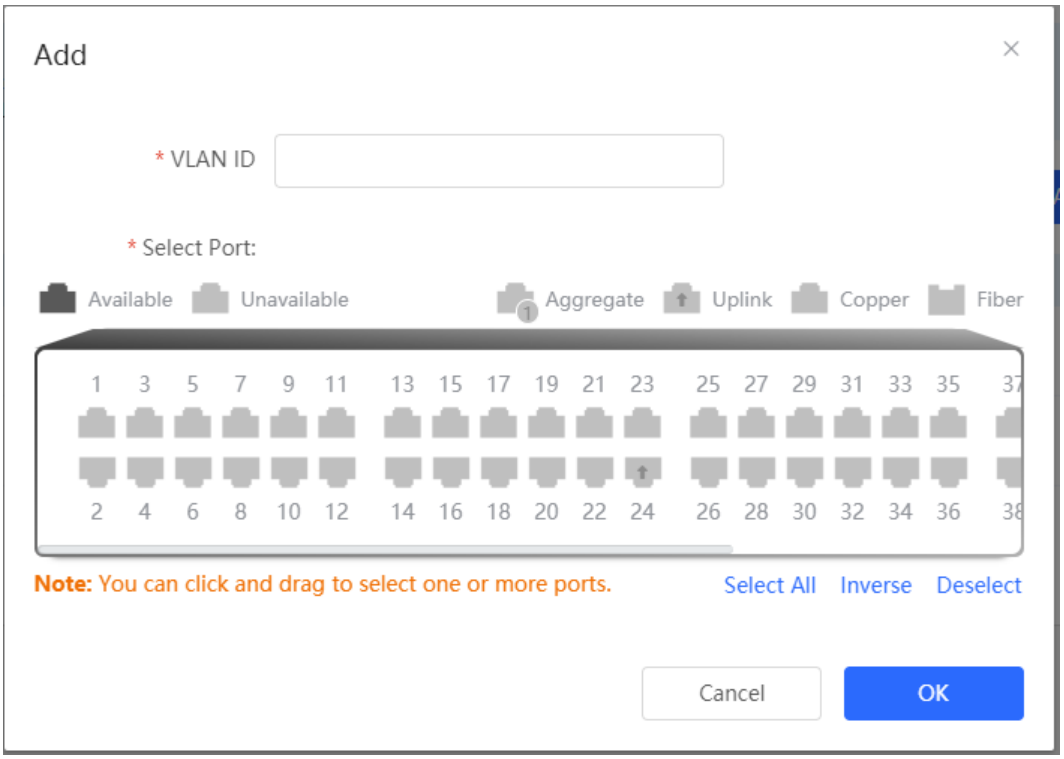
When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard.

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.





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 .

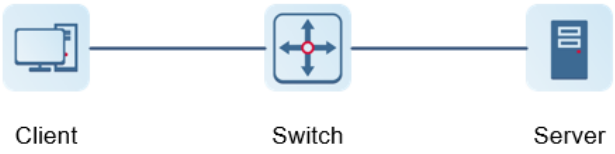
IEEE 802 LAN , as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN .

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.

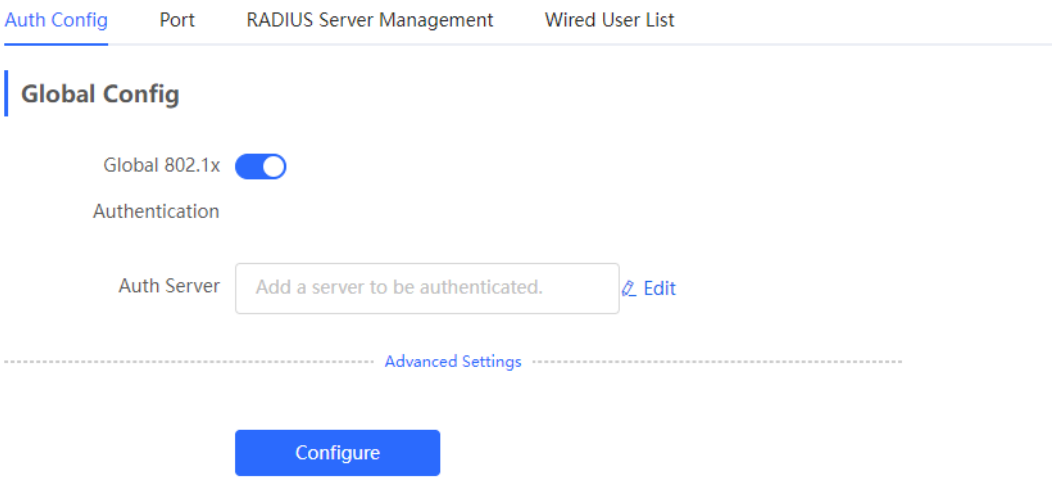
instruction

RG- NBS switching devices only support the authentication function.

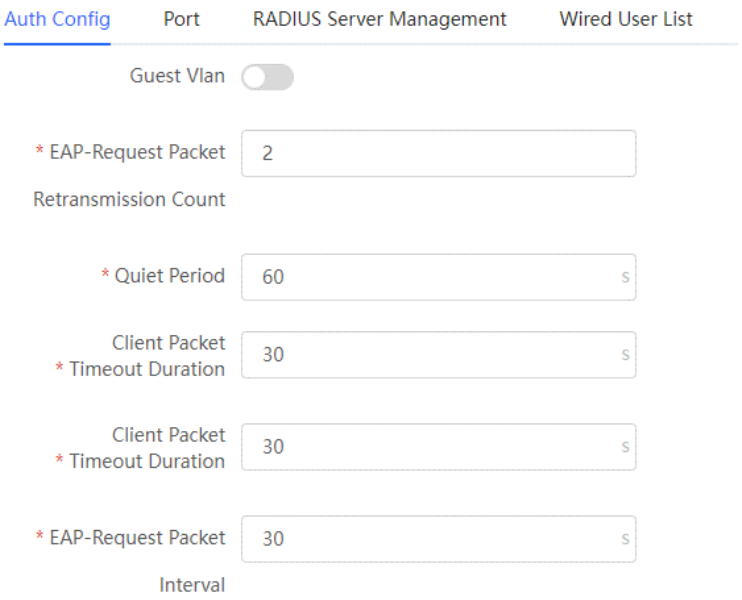
9.7.2 Configuration 802.1x

[Local Management - Page Wizard] Security > 802.1x Authentication > Auth Config

Click the " Global 802.1x " switch, the system prompts to confirm whether to enable it, click <Configure>.



Click Advanced Settings to configure parameters such as Guest VLAN .

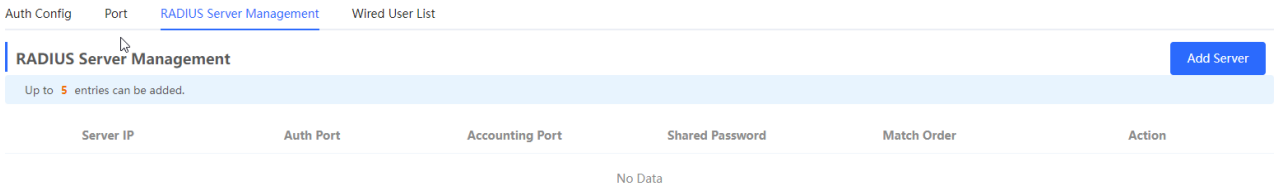


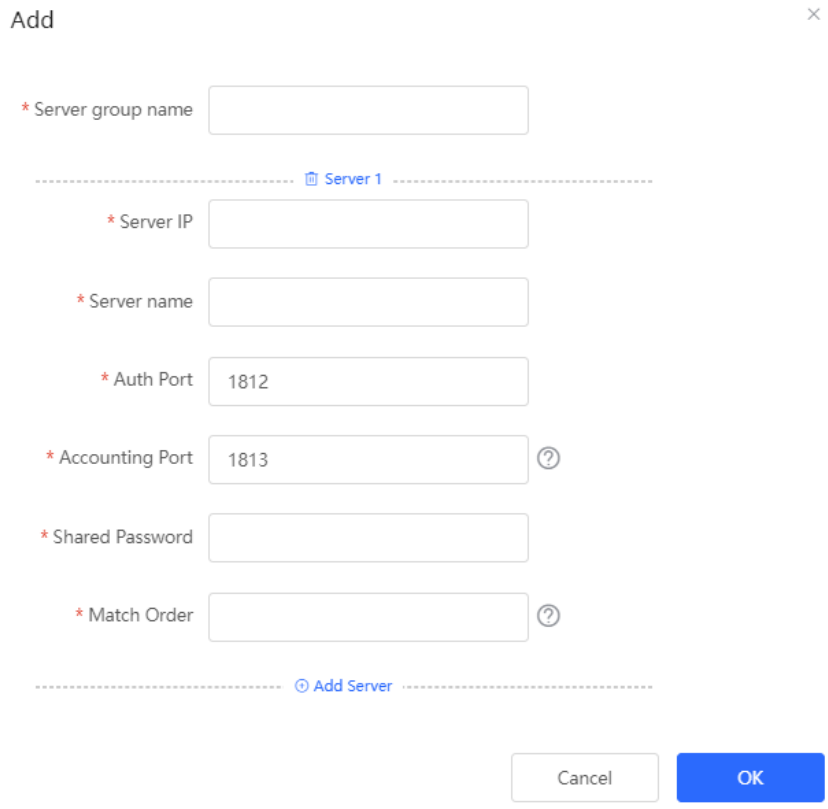
parameter	illustrate
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
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 :

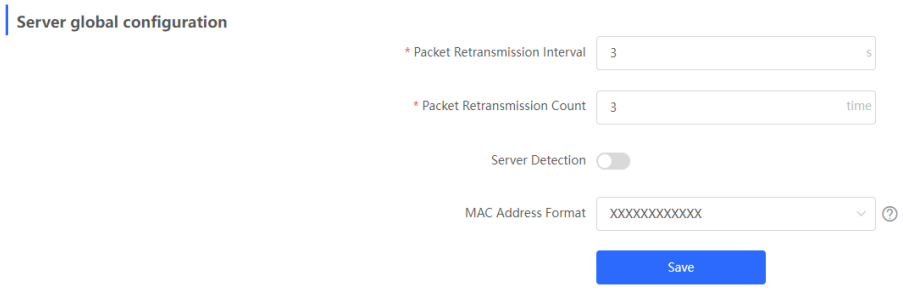
- The Radius server is fully built and configured as follows.
  - Add username and password for client login.
  - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
  - a trusted IP on the Radius server.
- The network connection between the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





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

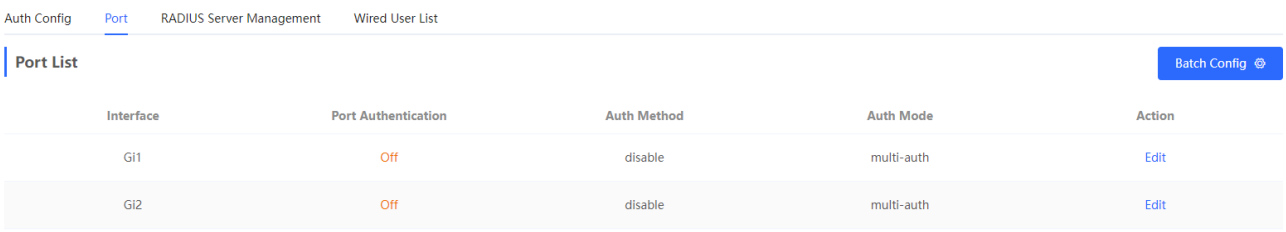
(3) Set up the server and click <Save> .

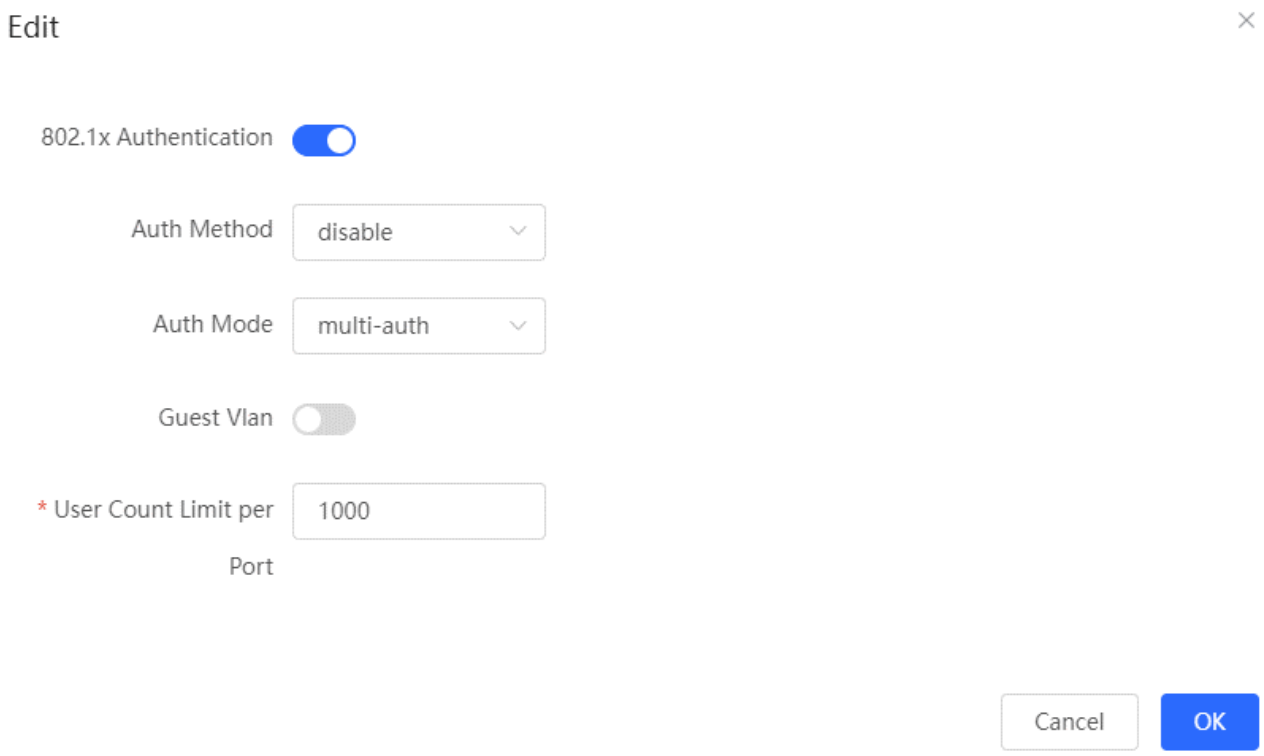


parameter	reference - do not translate	illustrate
Packet Retransmission Interval	packet retransmission interval	Configure the interval for the device to send request packets before confirming that there is no response from RADIUS
Packet Retransmission Count	Packet retransmission times	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS

parameter	reference - do not translate	illustrate
Server Detection	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	M AC 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) , eg 00d0f8aabbcc

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





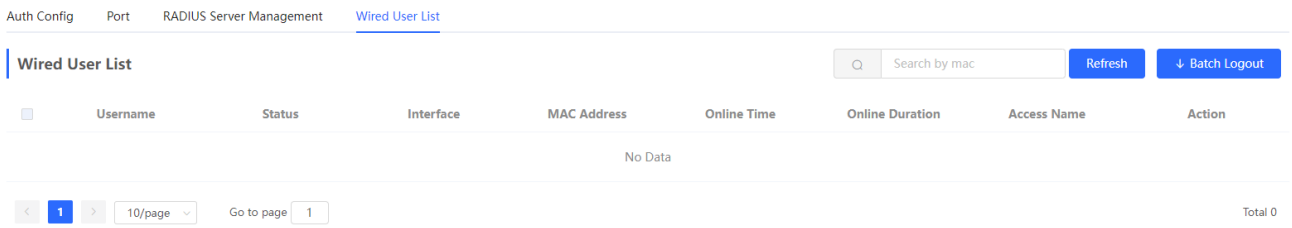
parameter	reference - do not translate	illustrate
802.1x Authentication	802.1x certification	When enabled, the selected interface will enable 8.02.1x authentication .
Auth Method	authentication method	disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication 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 .

parameter	reference - do not translate	illustrate
Auth Mode	authentication 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 Internet single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication
Guest Vlan	Guest VLAN	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN Notice 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	Maximum number of users per port	Limit the number of users under the interface Product Difference Description The value range of NBS3100 series switches is 1-256 , and other switches are 1-1000

9.7.3 View the list of wired authentication users

8.02.1x 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.

[Local Management - Page Wizard]Security Management >> 802.1x Authentication to obtain specific user information.



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

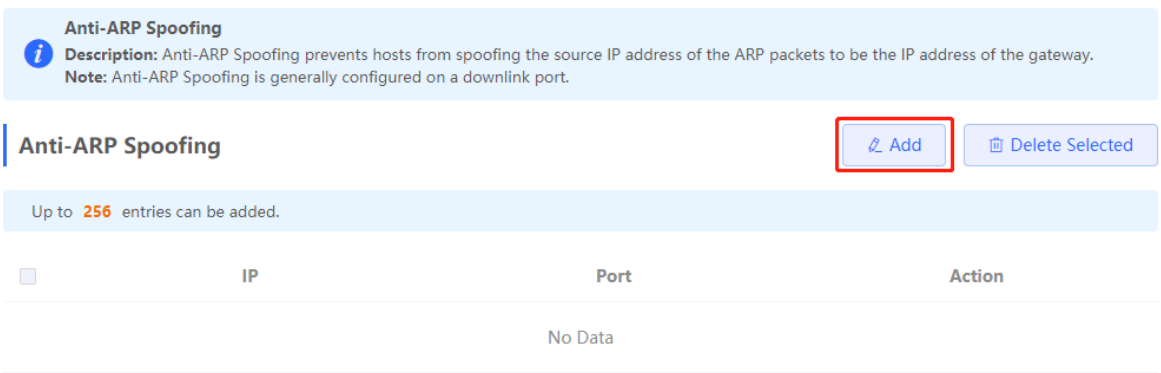
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

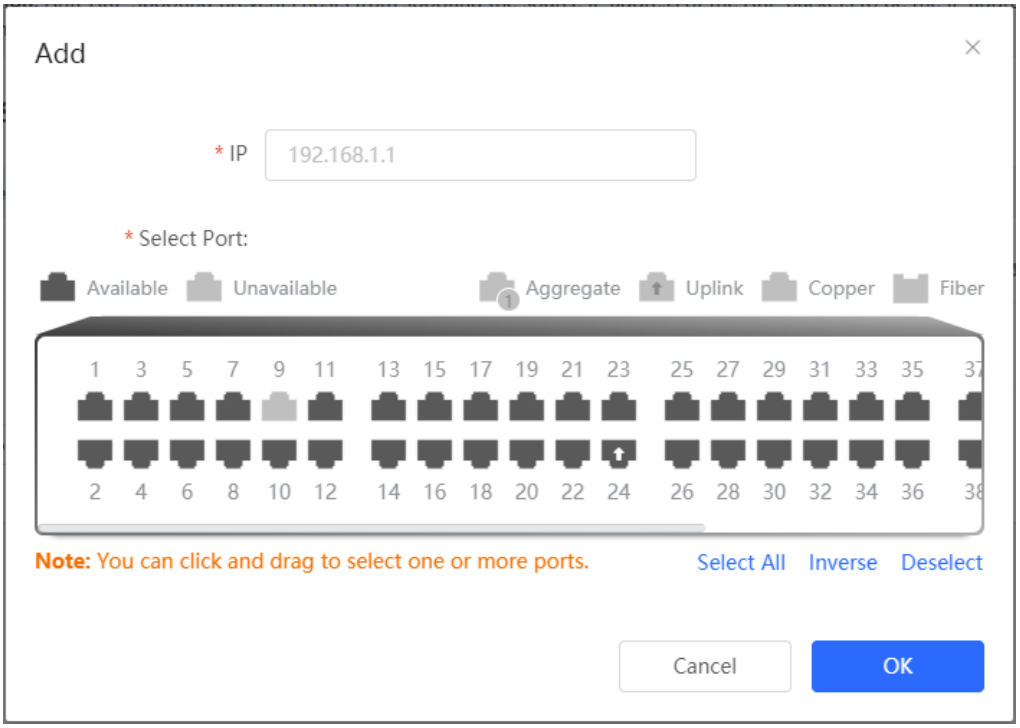
1. Enabling Anti-ARP Spoofing

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.

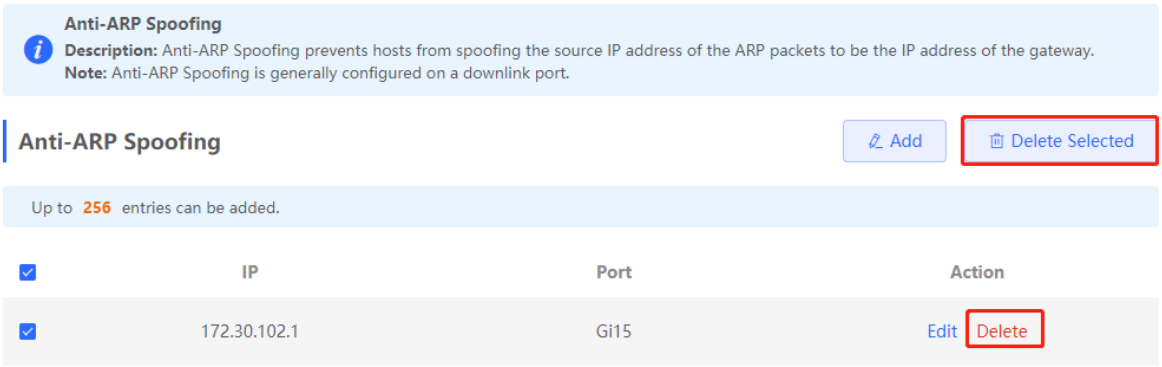




2. Disabling Anti-ARP Spoofing

Batch disable: Select an entry to be deleted in the list and click **Delete Selected**.

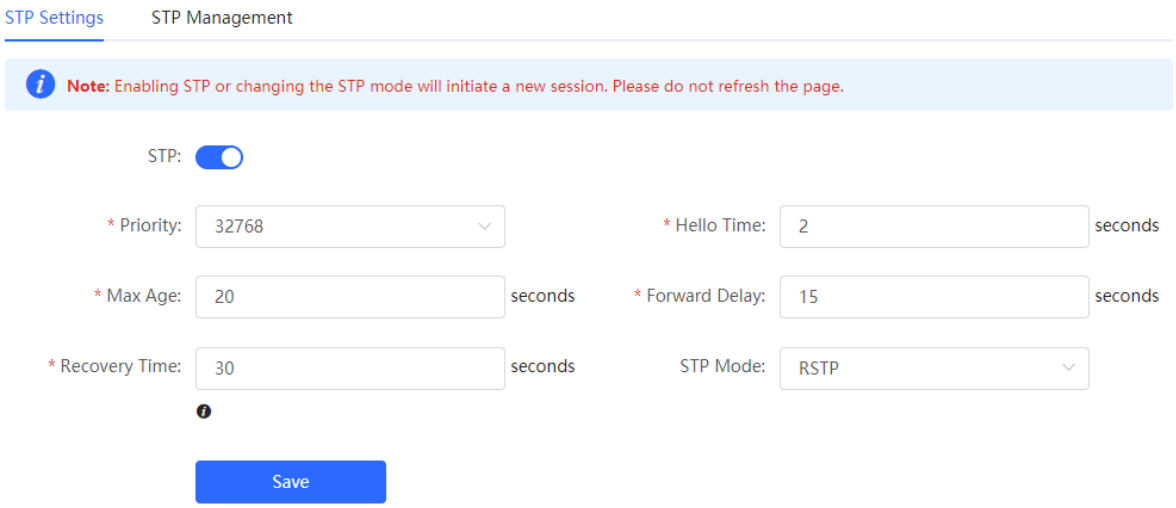
Disable one port: click **Delete** in the last **Action** column of the corresponding entry.



10 Advanced Configuration

10.1 STP

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



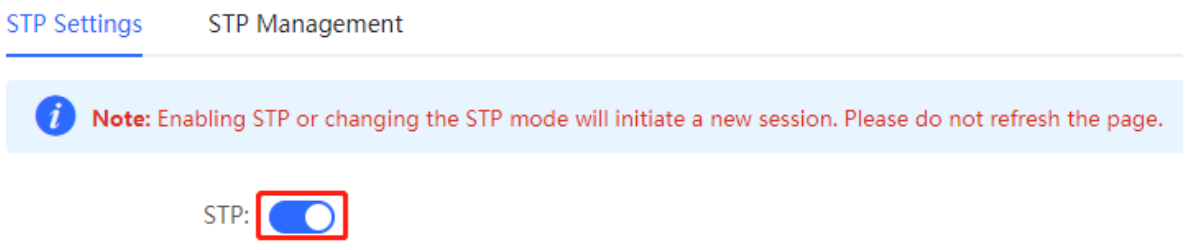
10.1.1 STP Global Settings

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

Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.



(2) Configure the STP global parameters, and click **Save**.

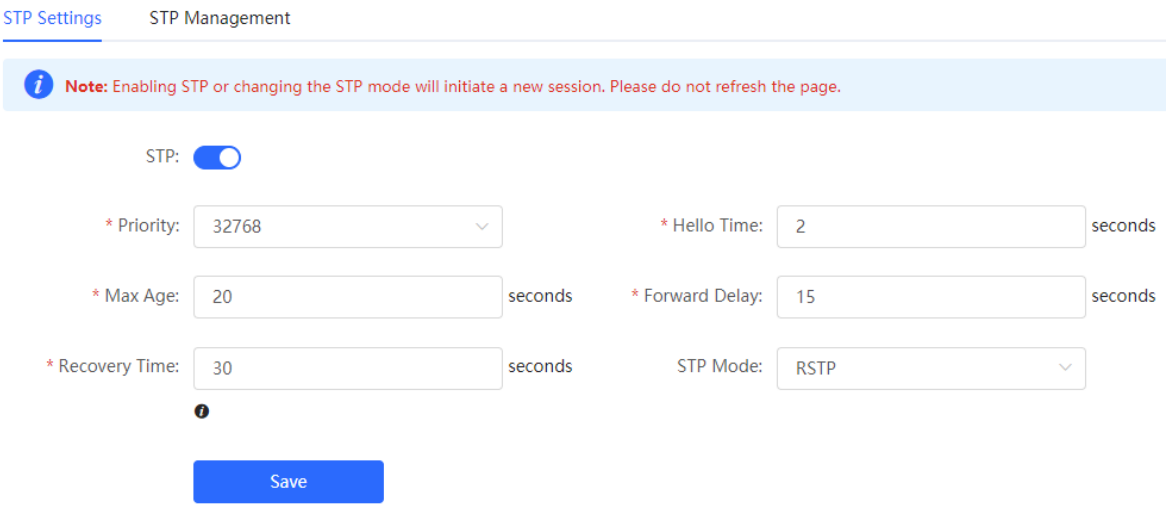


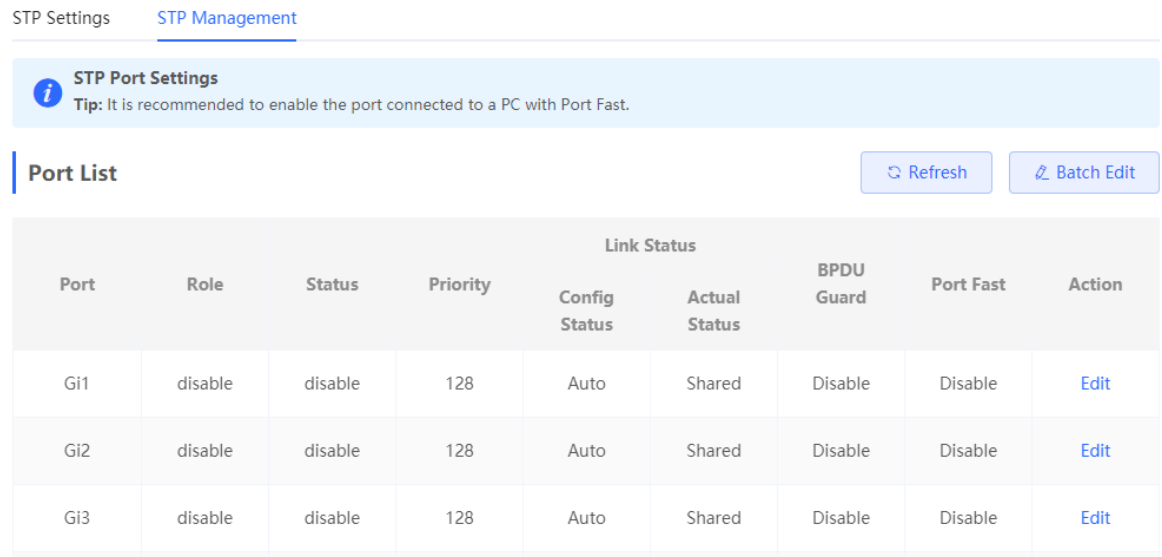
Table 10-1 Description of STP Global Configuration Parameters

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



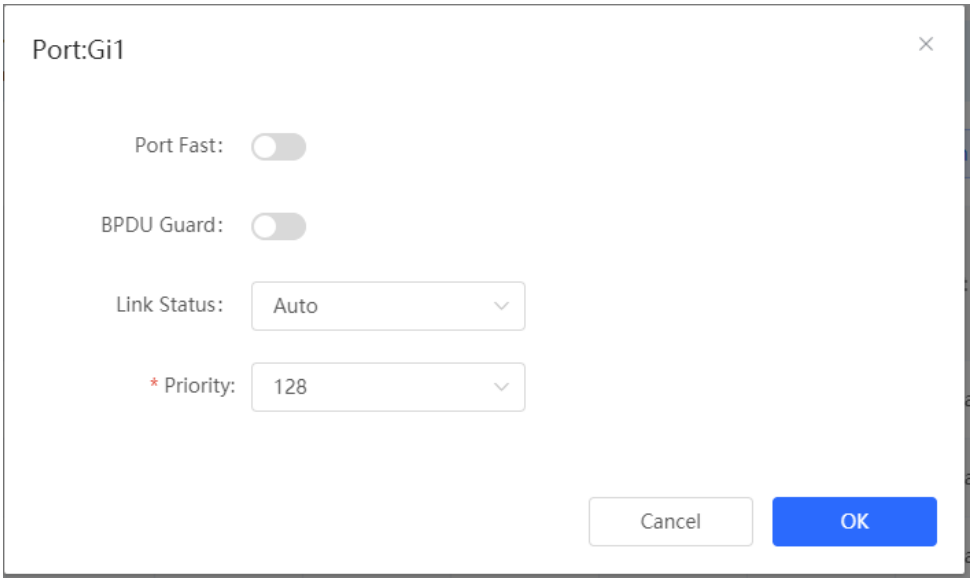


Table 10-2 Description of STP Configuration Parameters of Ports

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 a upstream bridge to a downstream device. ● Disable (blocked ports): Ports that have no effect in the spanning tree.	NA
Status	● Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. ● Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. ● Listening: If a port can become the root port or designated port, the port will enter the listening state. **Listening**: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. ● Learning: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. ● Forwarding: Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs.	NA
Priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Link Status Config 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	NA

Parameter	Description	Default Value
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

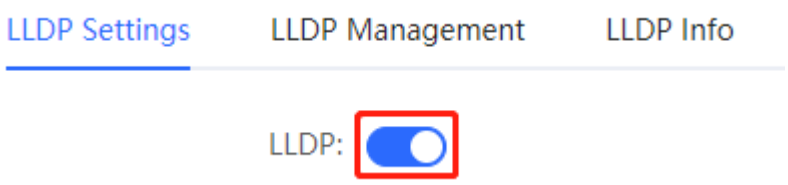
10.2.1 Overview

LLDP (Link Layer Discovery Protocol) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the Eweb management system can learn the topological connection status, for example, ports of the device that are connected to other devices, port rates at both ends of a link, and duplex mode matching status. An administrator can locate and troubleshoot faults quickly based on the preceding information.

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.



(2) Configure the global LLDP parameters and click **Save**.

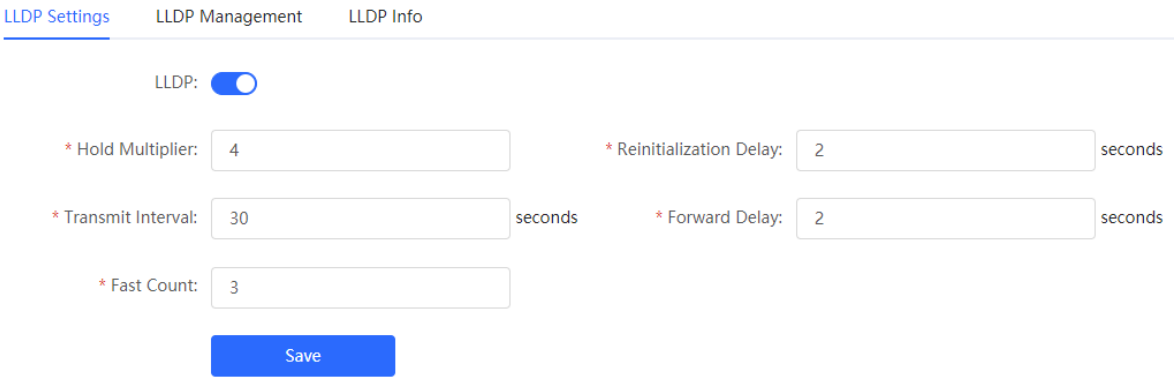


Table 10-3 Description of LLDP Global Configuration Parameters

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

Parameter	Description	Default Value
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

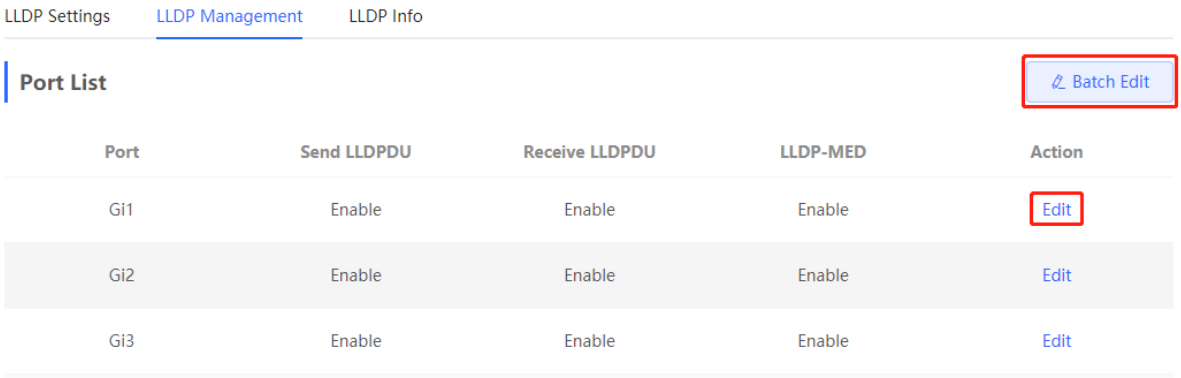
Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Management**.

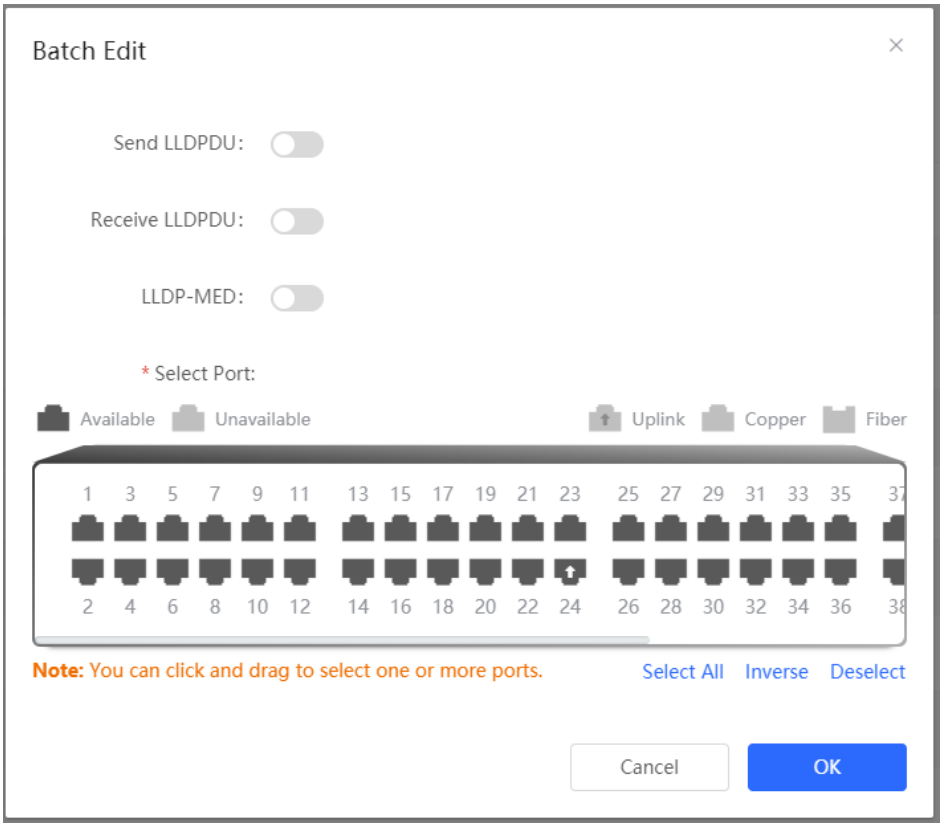
In **Port List**, Click **Edit** in the **Action** column, or click **Batch Edit**, select the desired port, configure the LLDP working mode on the port and whether to enable LLDP-MED, and click **OK**.

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).



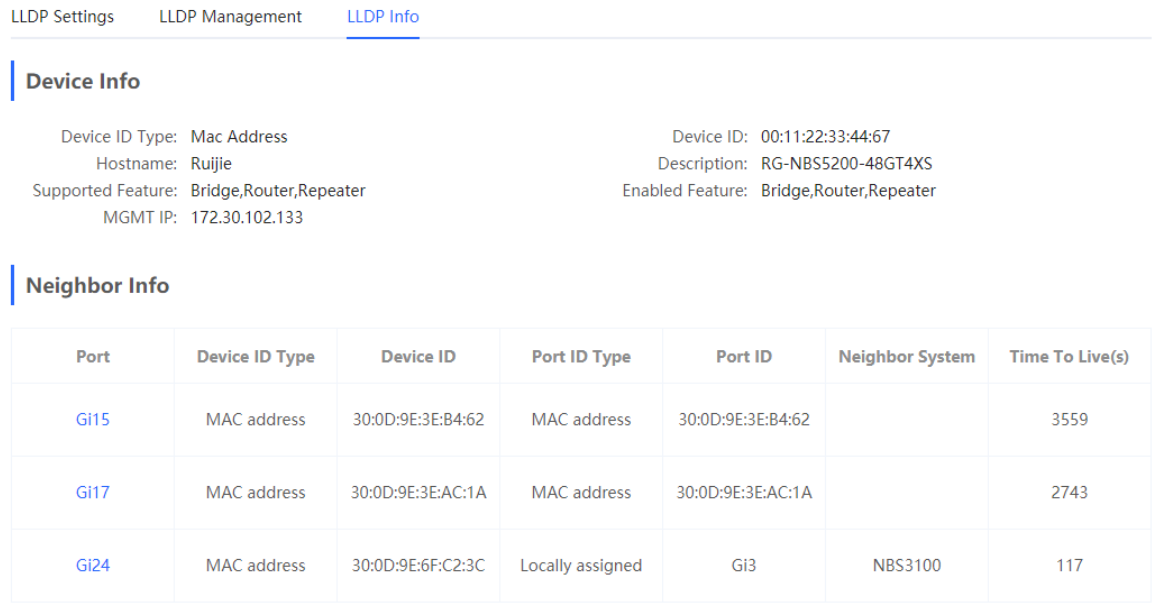


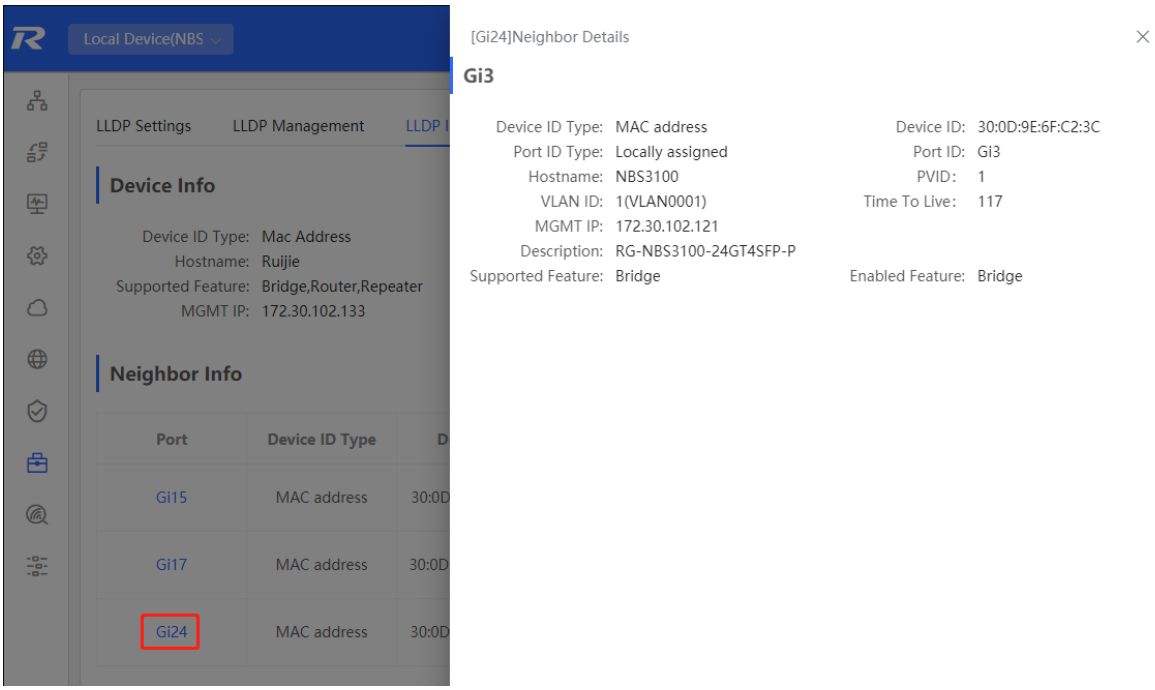
10.2.4 Displaying LLDP information

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 in the network topology. When an administrator configures the VLAN, port rate, duplex mode, an error will be prompted if the configurations do not match those on the connected neighbor.





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.

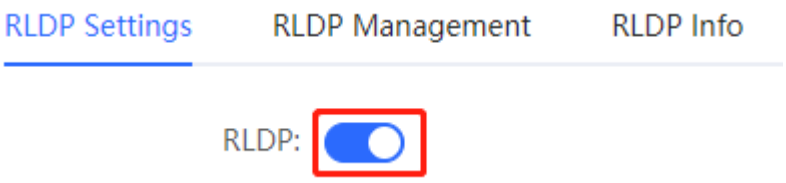
Supports enabling the RLDP function of the access switches in the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and the handling methods after a link fault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

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.



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

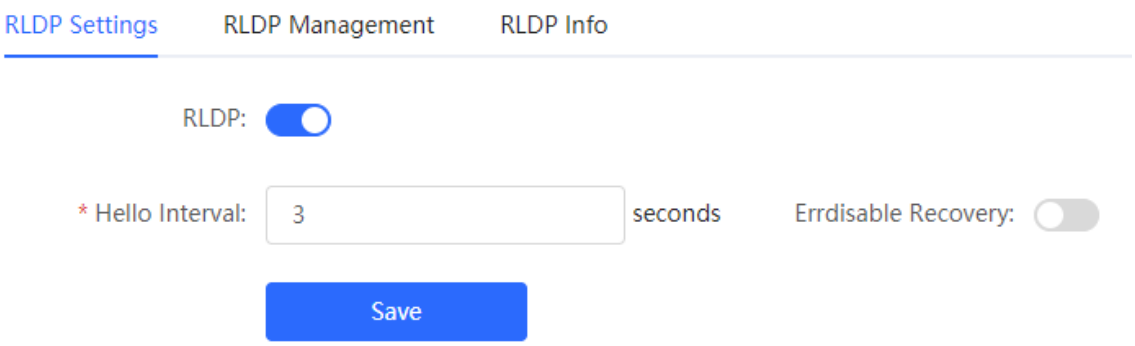


Table 10-4 Description of RLDP Global Configuration Parameters

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**.

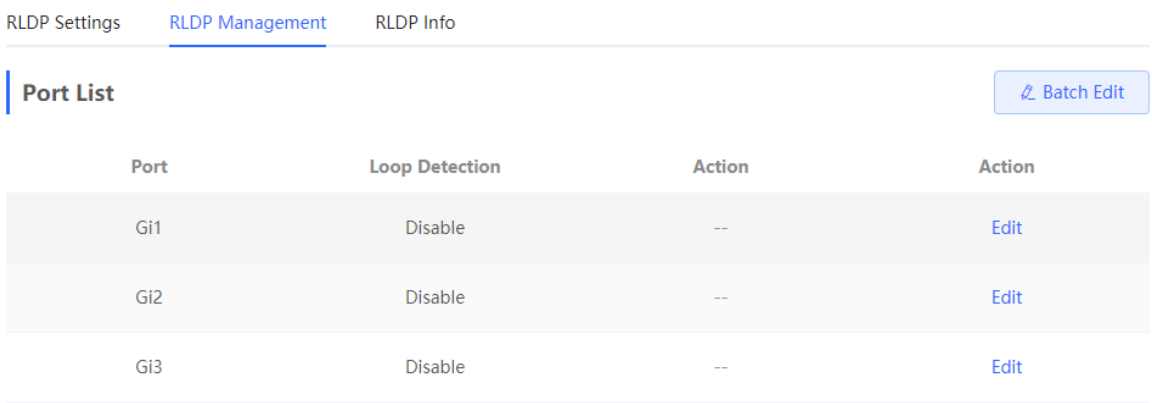
In **Port List,** click **Edit** in the Action column or click **Batch Edit**, select the desired port, configure whether to enable loop detection on the port and the handling method after a fault is detected, and click **OK**.

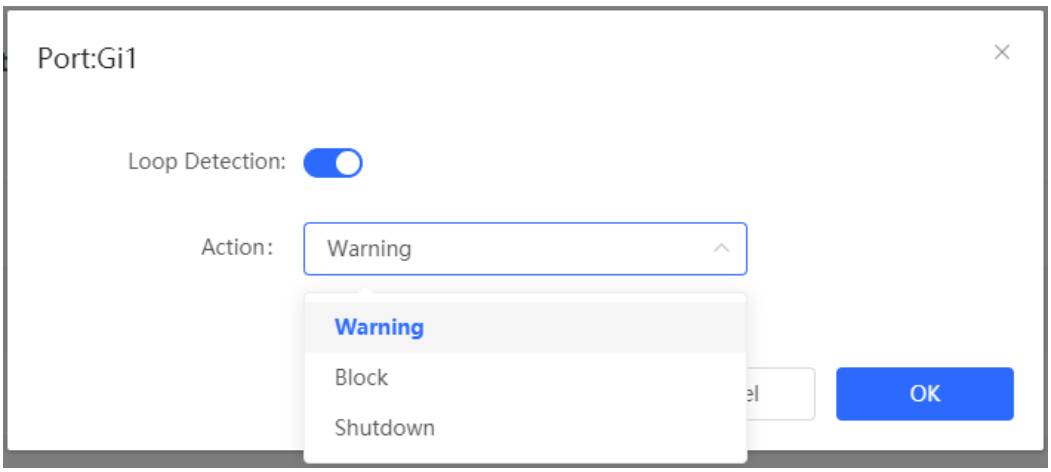
There are three methods to handle port failures:

- 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.

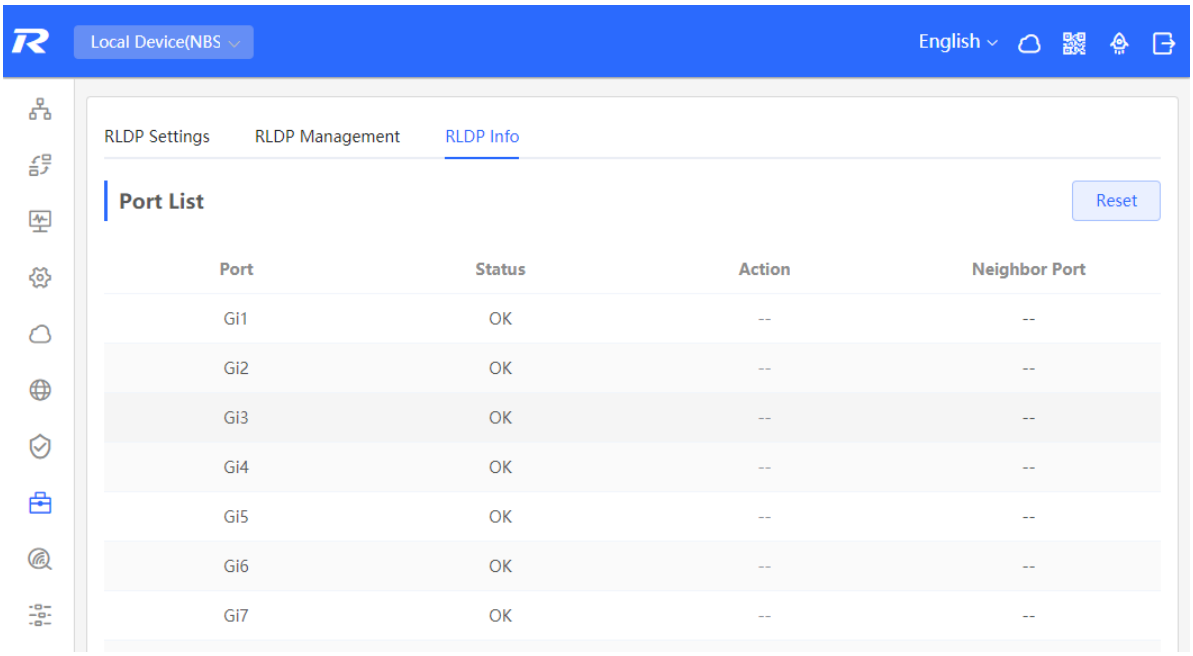




3. Displaying RLDP information

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

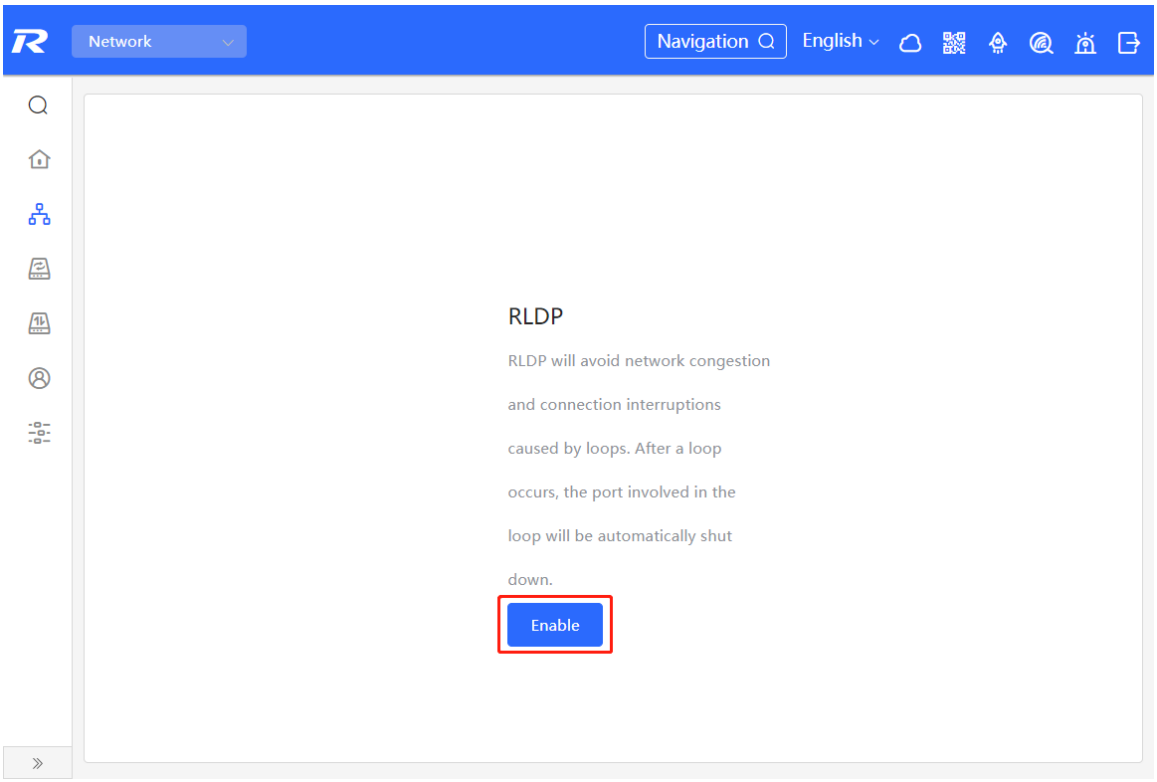
You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDP status triggered by a port to the normal state.



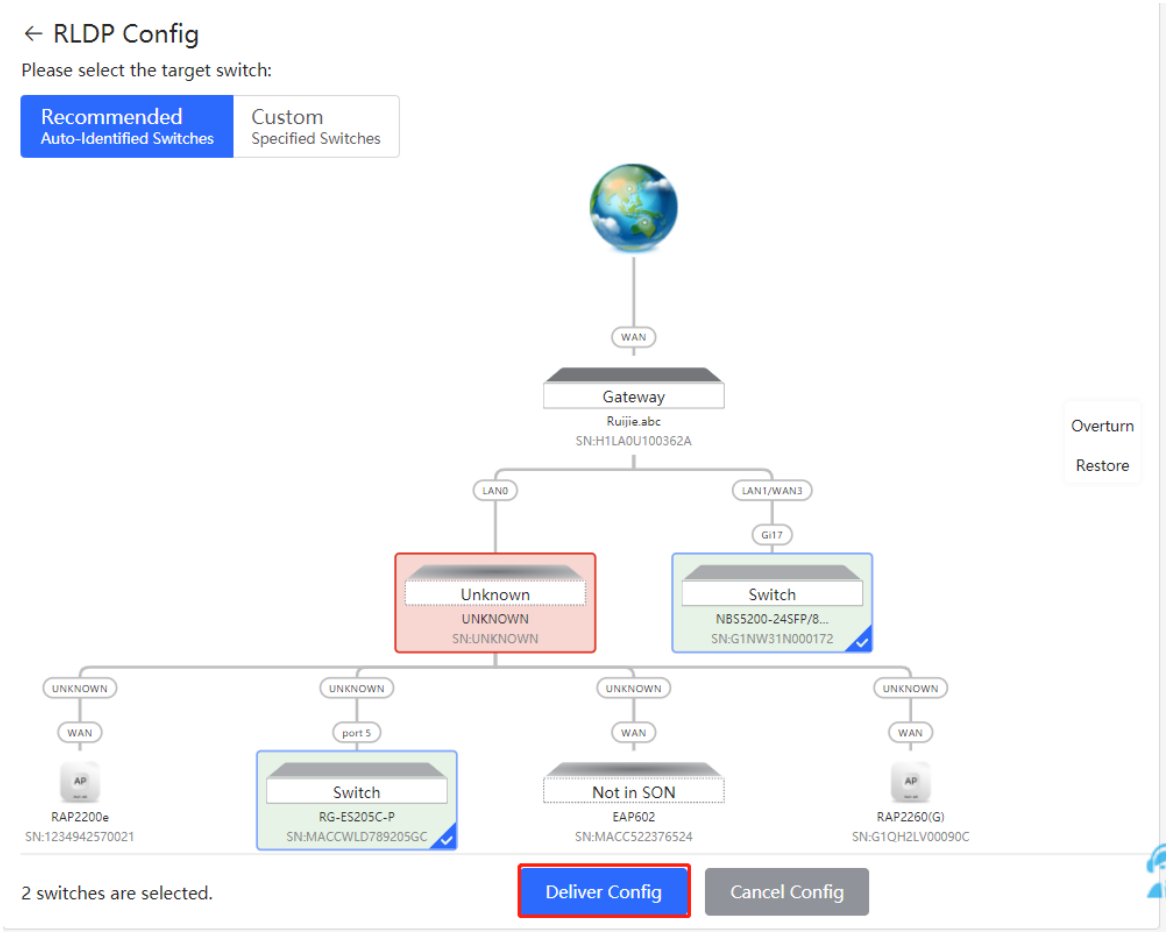
10.3.3 Batch Configuring Network Switches

Choose **Network** > **RLDP**.

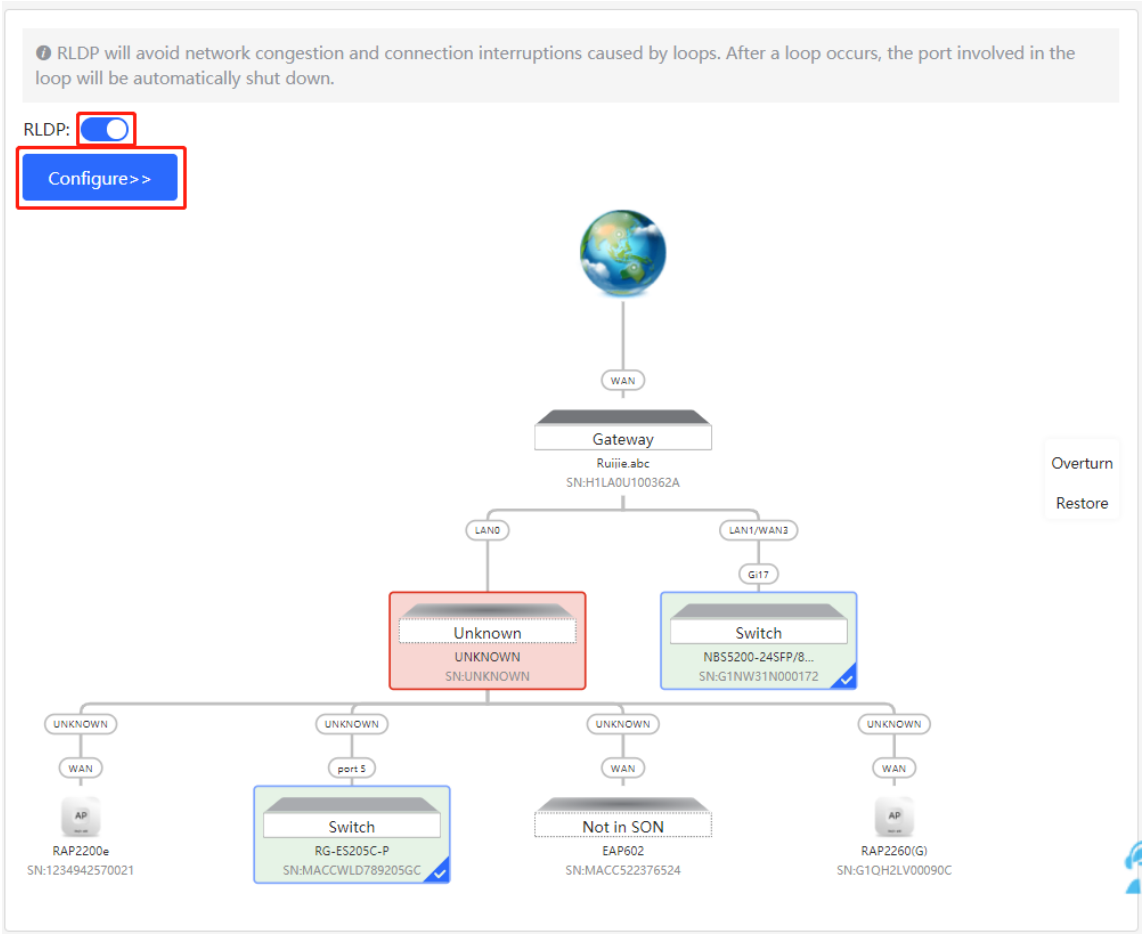
(1) Click **Enable** to access the **RLDP Config** page.



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



(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.

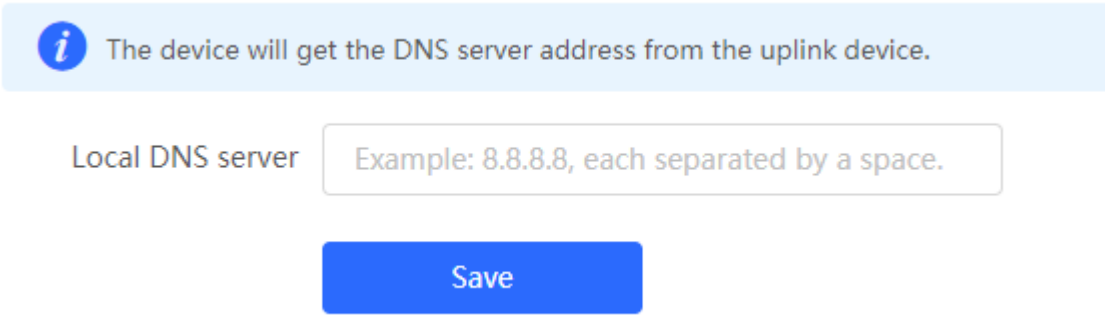


10.4 Configuring the Local DNS

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.



10.5 Voice VLAN

Caution

The Voice VLAN function is supported by RG-NBS3100 Series, RG-NBS3200 Series, RG-NBS5100 Series and RG-NBS5200 Series Switches.

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**.

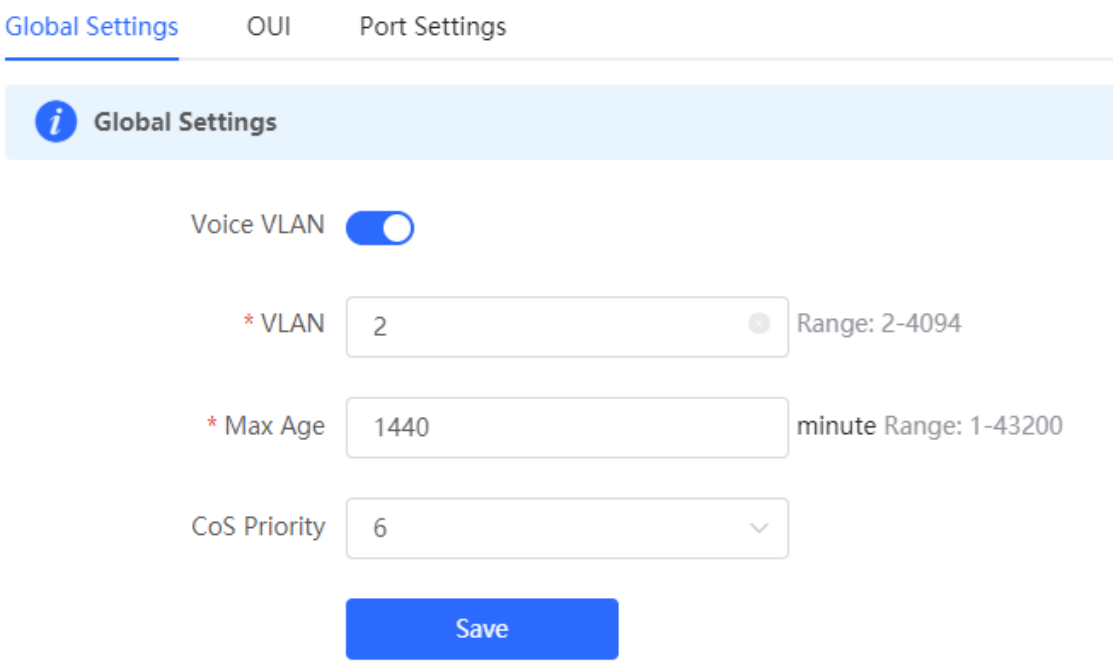


Table 10-5 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable
VLAN	VLAN ID as Voice VLAN	NA

Parameter	Description	Default Value
Max Age	Aging time of voice VLAN, in minutes. In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN	1440 minutes
CoS Priority	The L2 Priority of voice stream packets in a Voice VLAN. The value range is from 0 to 7. A greater value indicates a higher priority. You can modify the priority of the voice traffic to improve the call quality.	6

10.5.3 Configuring a Voice VLAN OUI

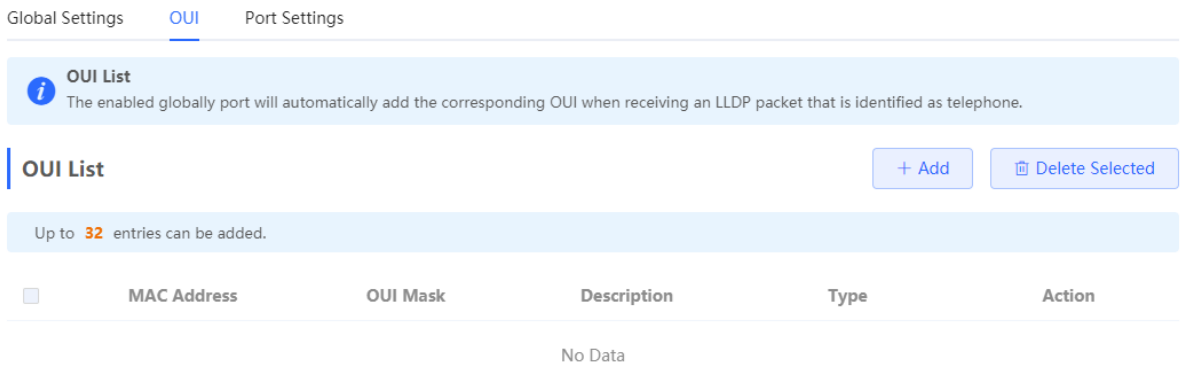
Choose **Local Device** > **Advanced** > **Voice VLAN** > **OUI**.

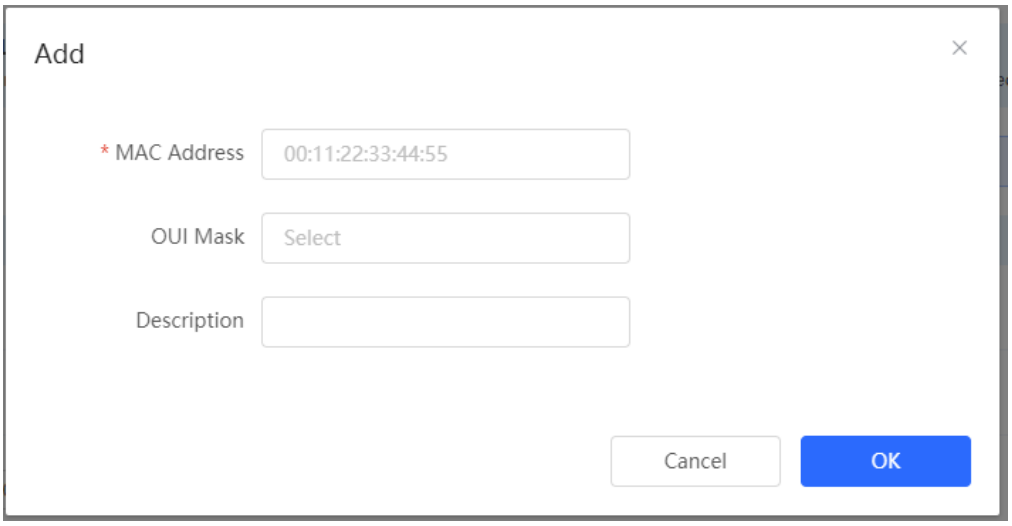
The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and sends them 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**.

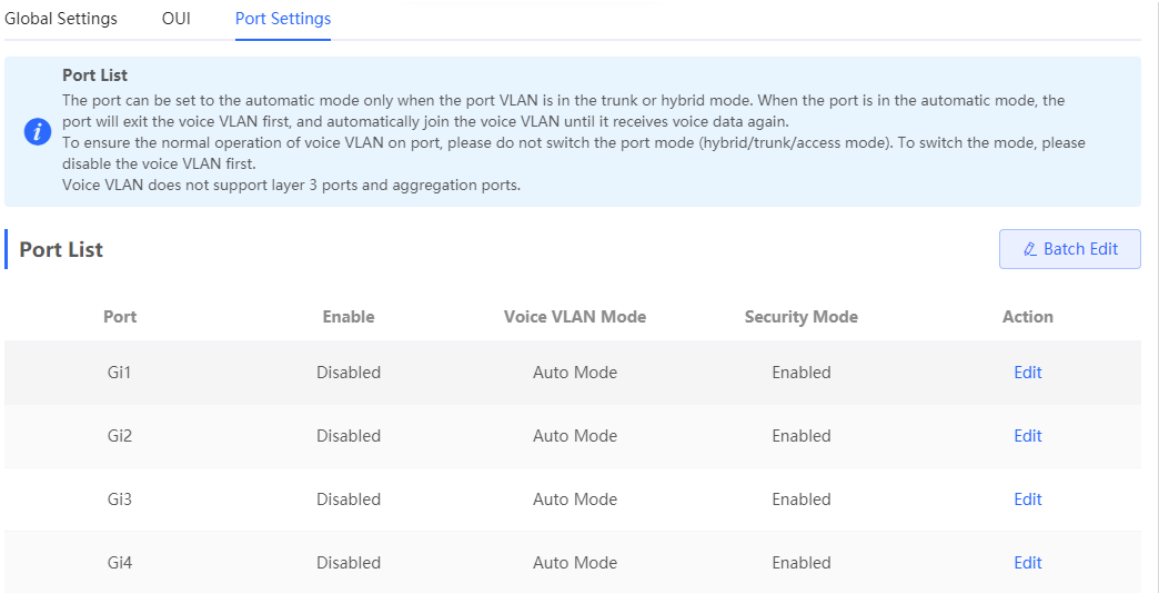




10.5.4 Configuring the Voice VLAN Function on a Port

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**.



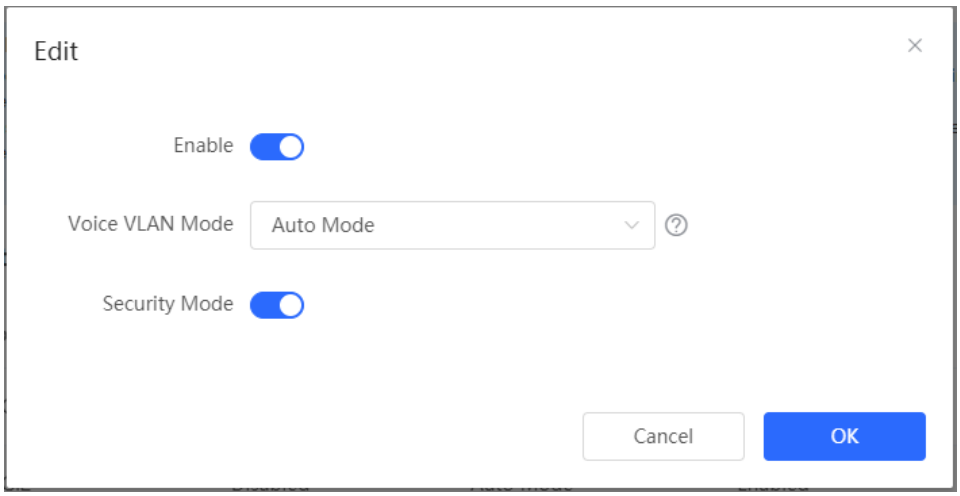


Table 10-6 Description of the Voice VLAN Configuration Parameters on a Port

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.

10.6 Configuring Smart Hot Standby (VCS)

Smart hot standby enables multiple switches to act as a hot standby device for each other, ensuring uninterrupted data forwarding in the event of a single point failure.

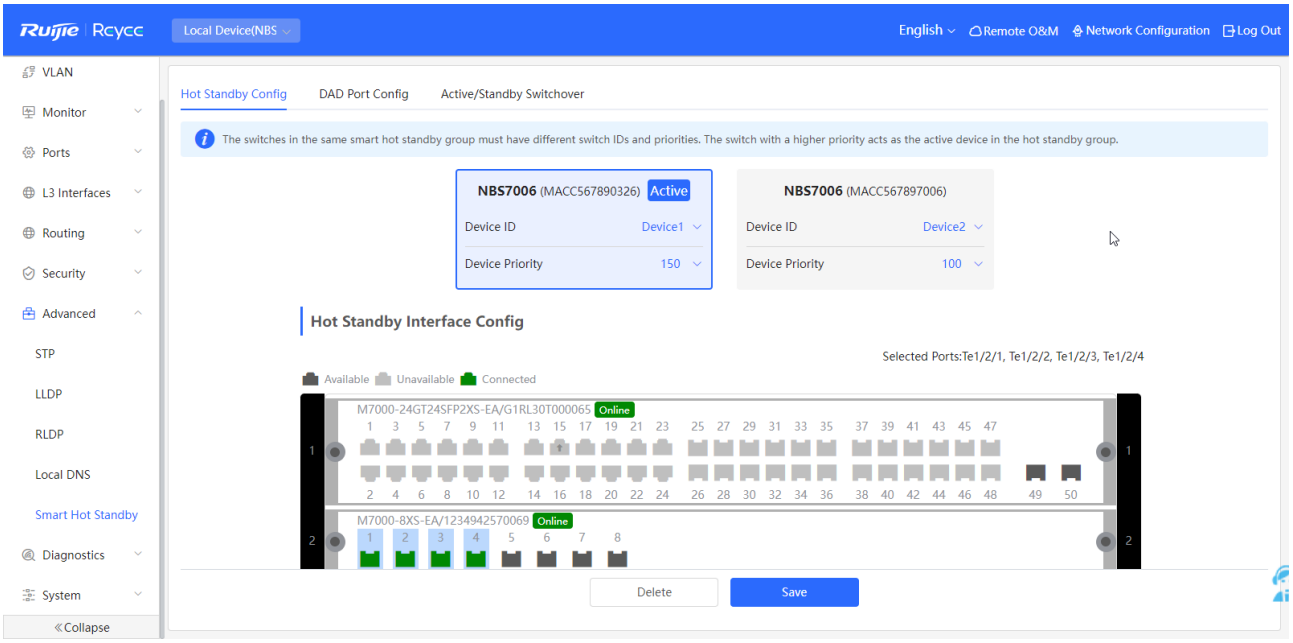
10.6.1 Configuring Hot Standby

View or modify selected hot standby interfaces, device IDs and priorities. The switch with a higher priority is elected as the active switch in a hot standby group.

Caution

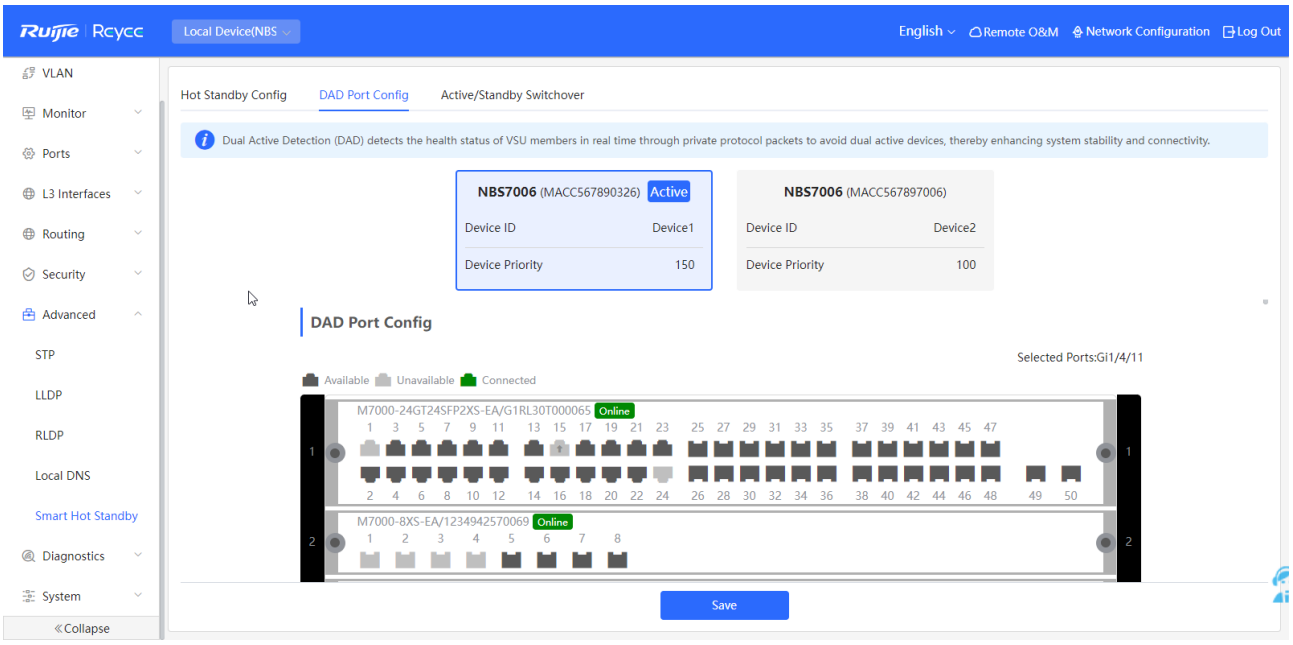
The devices in a hot standby group must have unique device IDs and priorities configured.

Choose **Local Device** > **Advanced** > **Smart Hot Standby**.



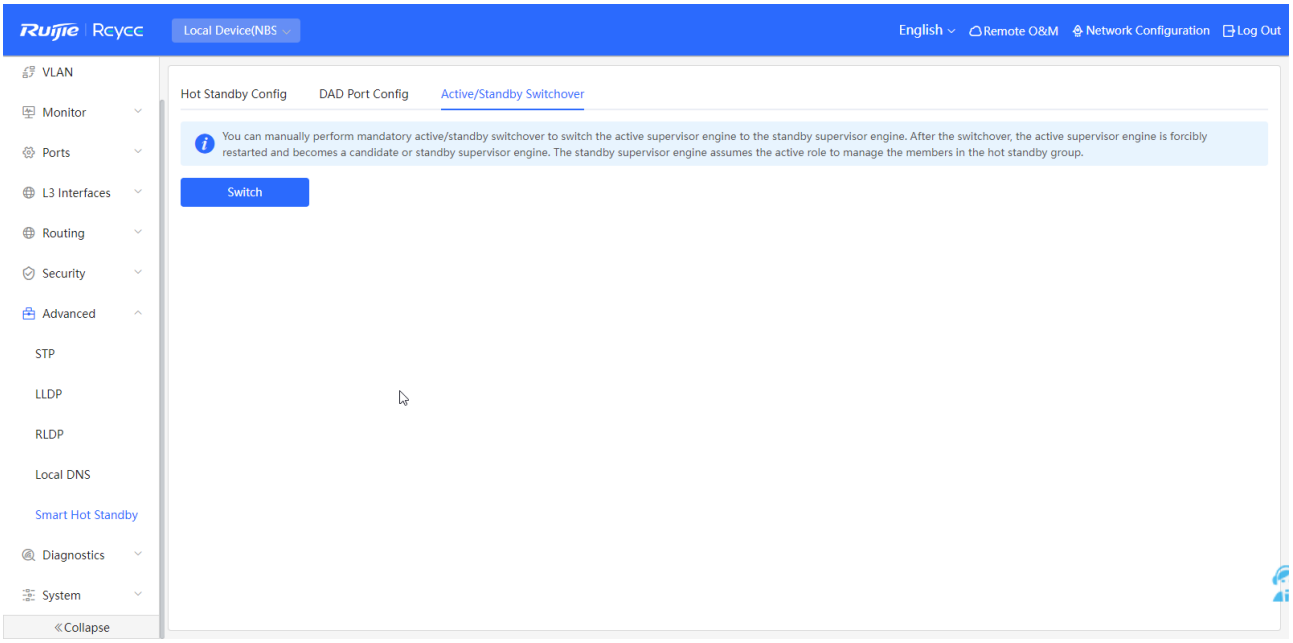
10.6.2 Configuring DAD Interfaces

After selecting the DAD interfaces of both the active and standby switches, connect these DAD interfaces with a network cable to prevent network failures caused by dual active devices.



10.6.3 Active/Standby Switchover

Active/Standby Switchover allow manual switching between the active and standby supervisor engines. Clicking the **Switch** button will restart the supervisor engine. Please exercise caution.

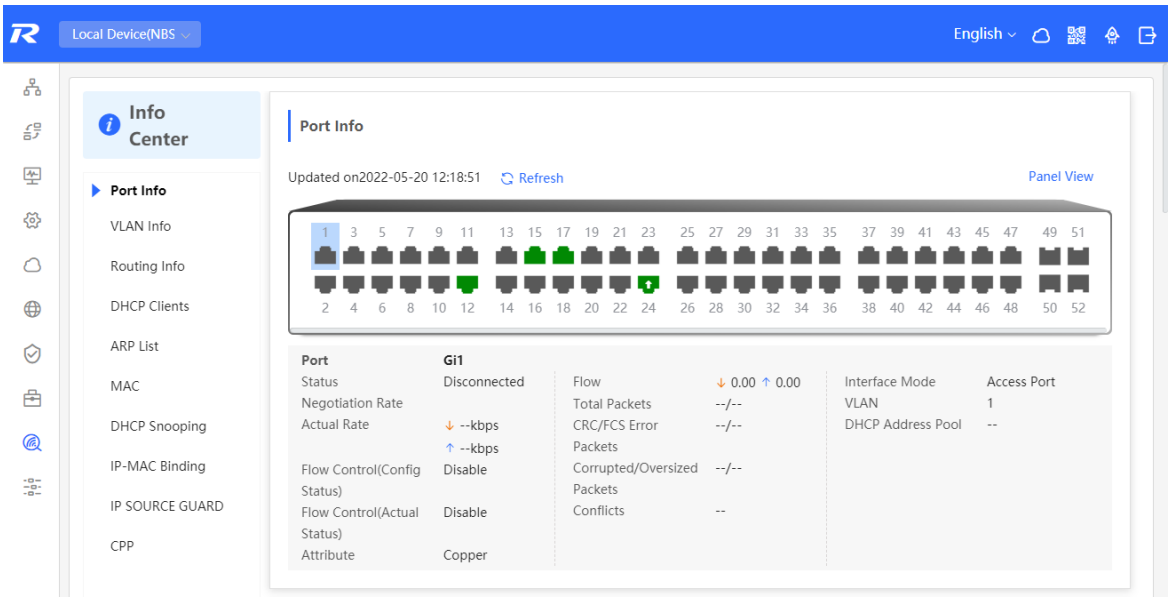


11 Diagnostics

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.



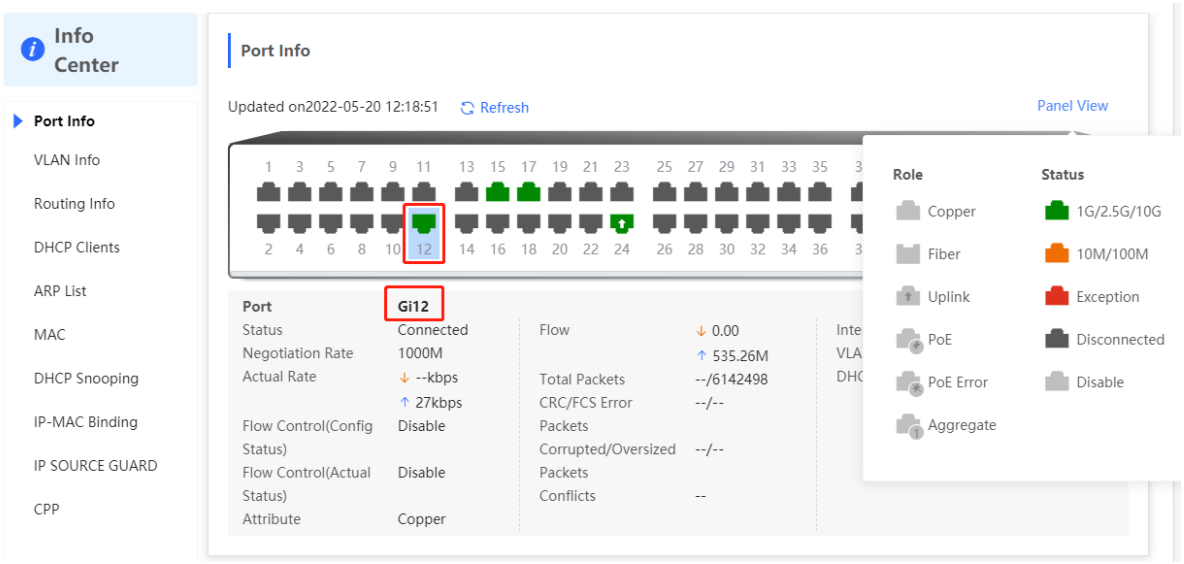
11.1.1 Port Info

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 4.2.
- To configure the L2 mode of the port and the VLAN to which it belongs, see 3.5.3.



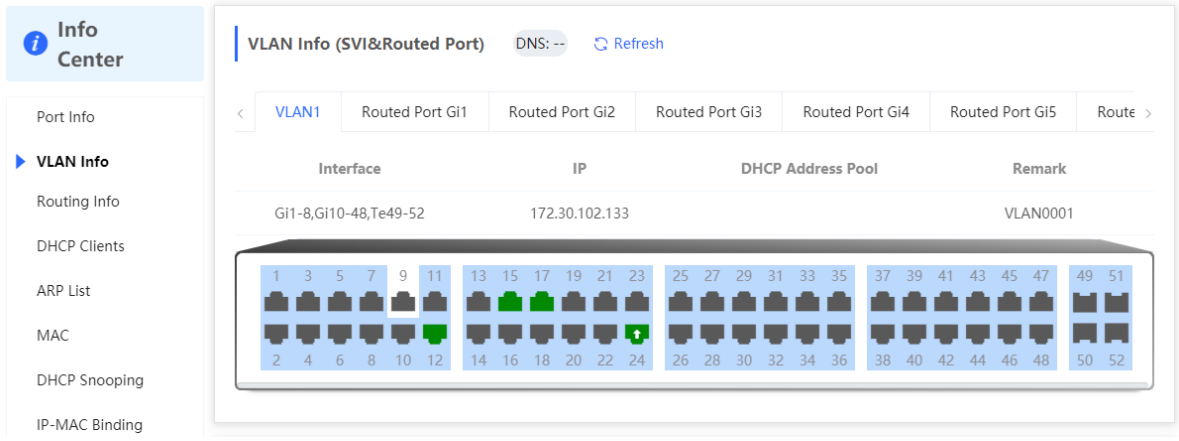
11.1.2 VLAN Info

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 3.5 .
- To configure SVI ports and routed ports, see 6.1.



11.1.3 Routing Info

Caution

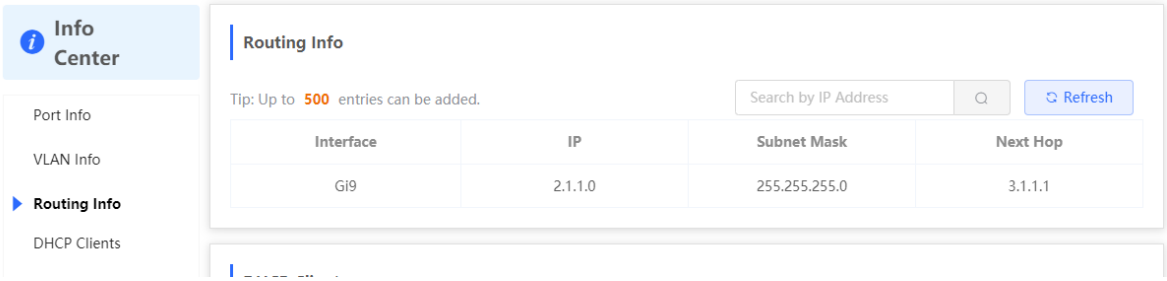
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

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

Displays the routing information on the device. The search box in the upper-right corner supports finding route entries based on IP addresses.

Note

To set up static routes, see 6.3.



11.1.4 DHCP Clients

Caution

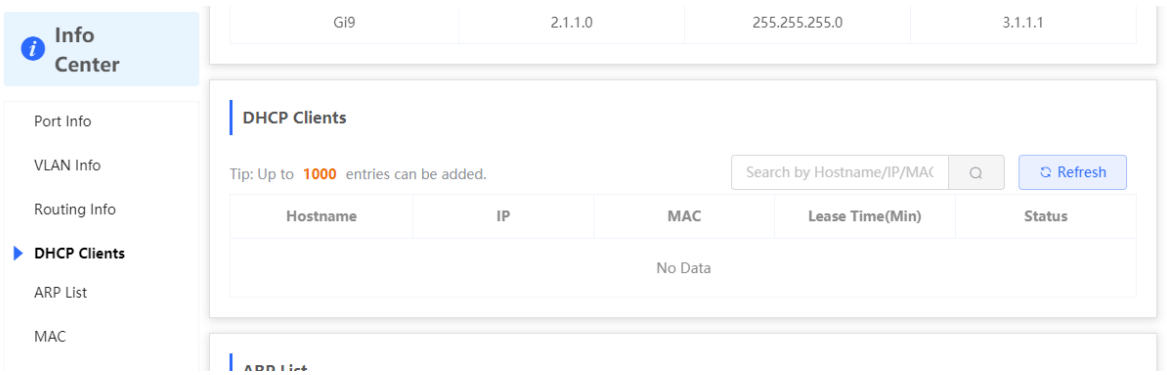
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Clients**.

Displays the IP address information assigned to endpoints by the device as a DHCP server.

Note

To configure DHCP server related functions, see 6.2.



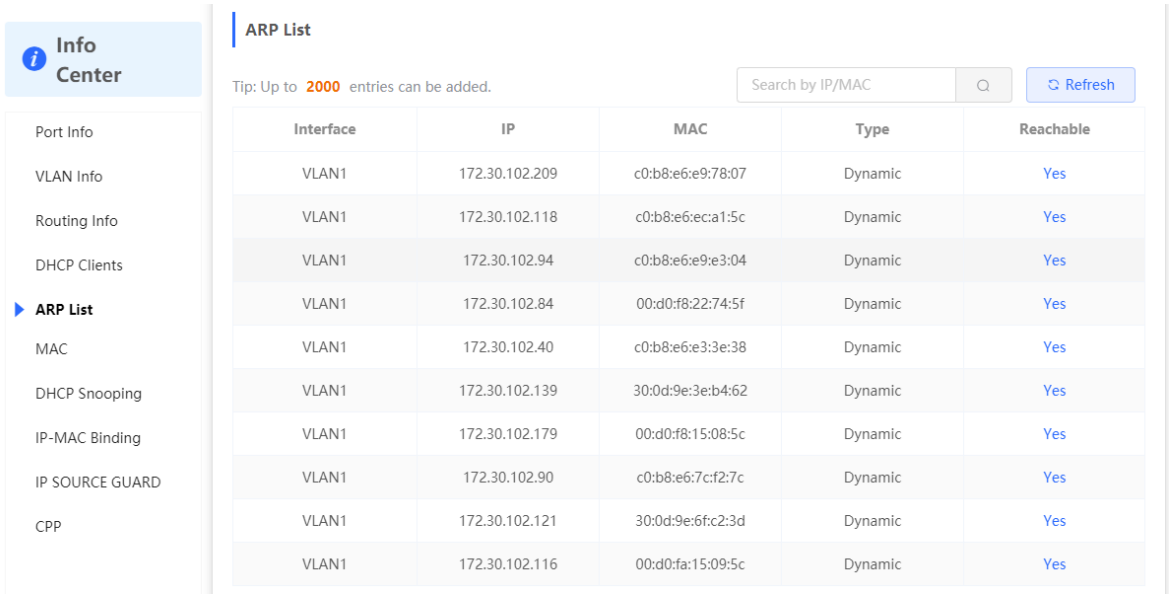
11.1.5 ARP List

Choose **Local Device** > **Diagnostics** > **Info Center** > **ARP List**.

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

Note

To bind dynamic ARP or manually configure static ARP, see 6.4.



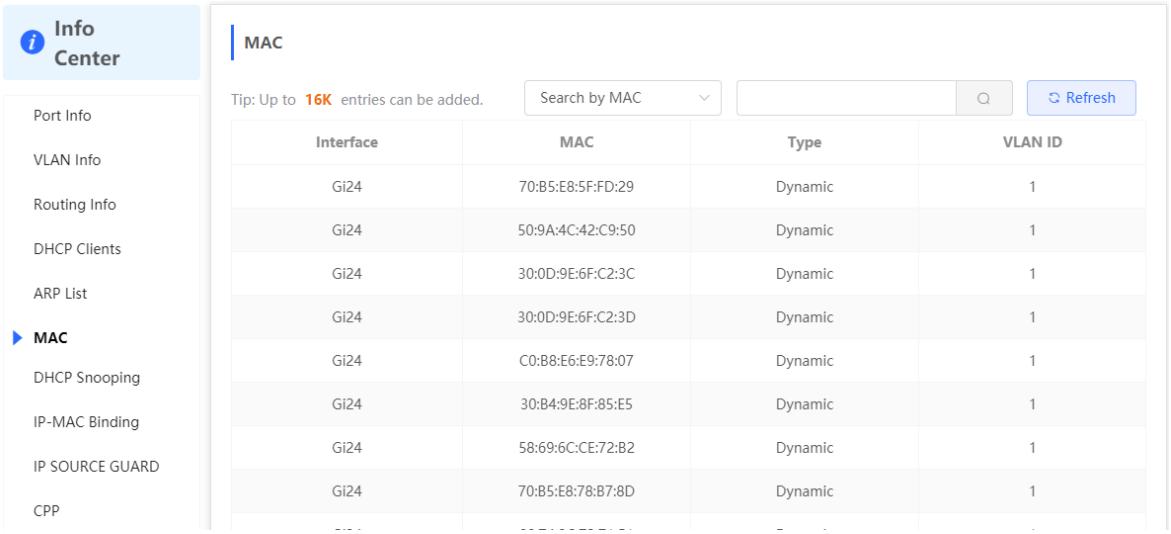
11.1.6 MAC Address

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

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

Note

To configure and manage the MAC address, see 3.3.



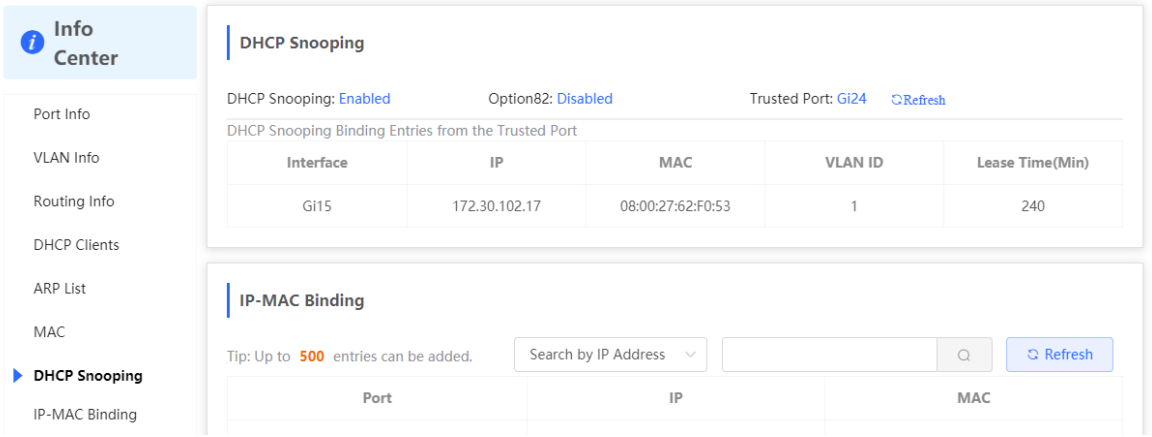
11.1.7 DHCP Snooping

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Snooping**.

Displays the current configuration of the DHCP snooping function and the user information dynamically learned by the trust port.

Note

To modify DHCP Snooping related configuration, see 7.1.



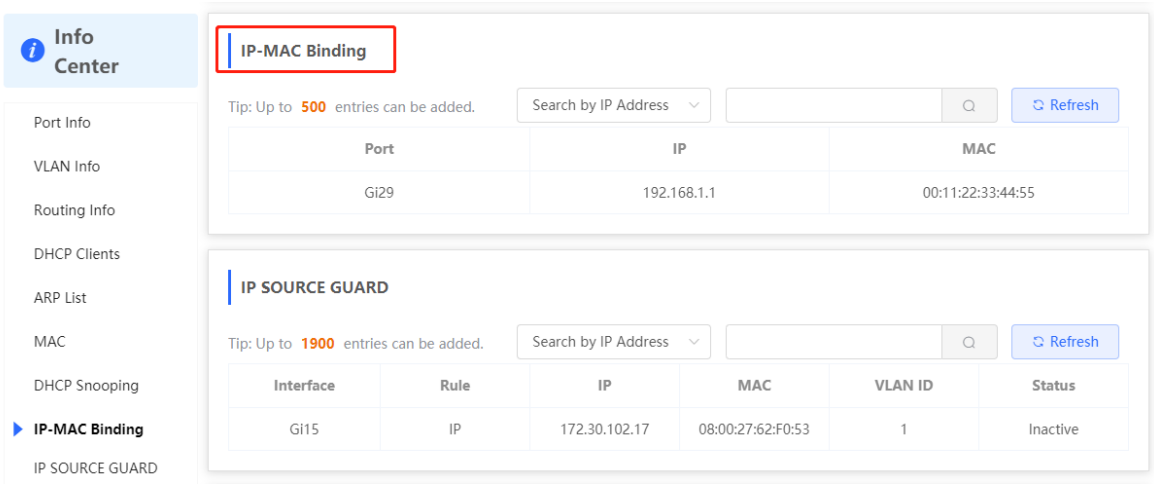
11.1.8 IP-MAC Binding

Choose **Local Device** > **Diagnostics** > **Info Center** > **IP-MAC Binding**.

Displays the configured IP-MAC binding entries. The device checks whether the source IP addresses and source MAC addresses of IP packets match those configured for the device and filters out IP packets not matching the binding.

Note

To add or modify the IP-MAC binding, see 7.5.



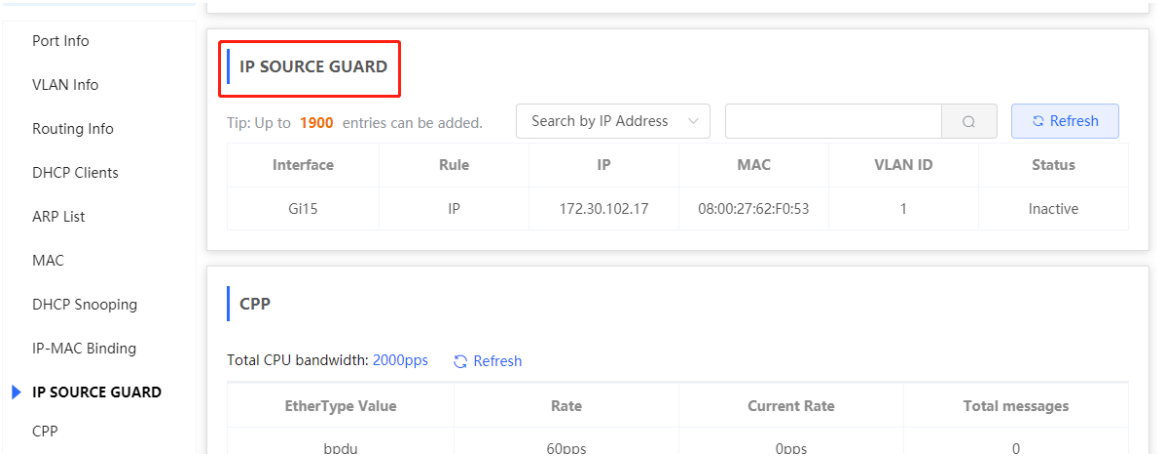
11.1.9 IP Source Guard

Choose **Local Device** > **Diagnostics** > **Info Center** > **Source Guard**.

Displays the binding list of the IP Source Guard function. The IP Source Guard function will check the IP packets from non-DHCP trusted ports according to the list, and filter out the IP packets that are not in the binding list.

Note

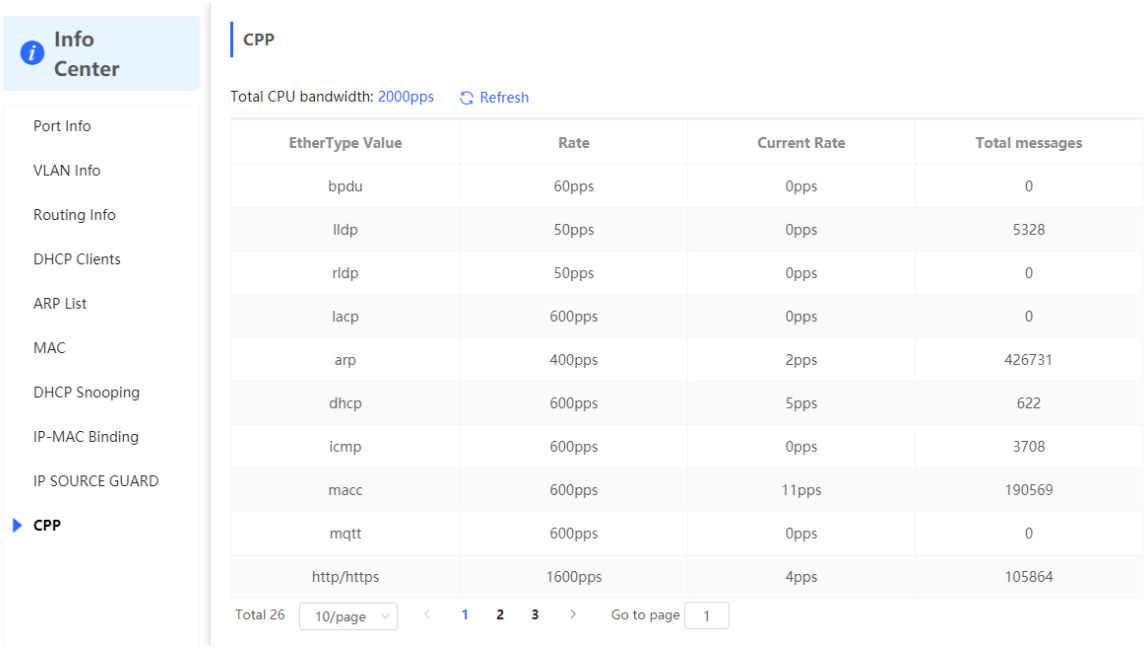
To configure IP Source Guard function, see 7.6.



11.1.10 CPP Info

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

Displays the current total CPU bandwidth and statistics of various packet types, including the bandwidth, current rate, and total number of packets.



11.2 Network Tools

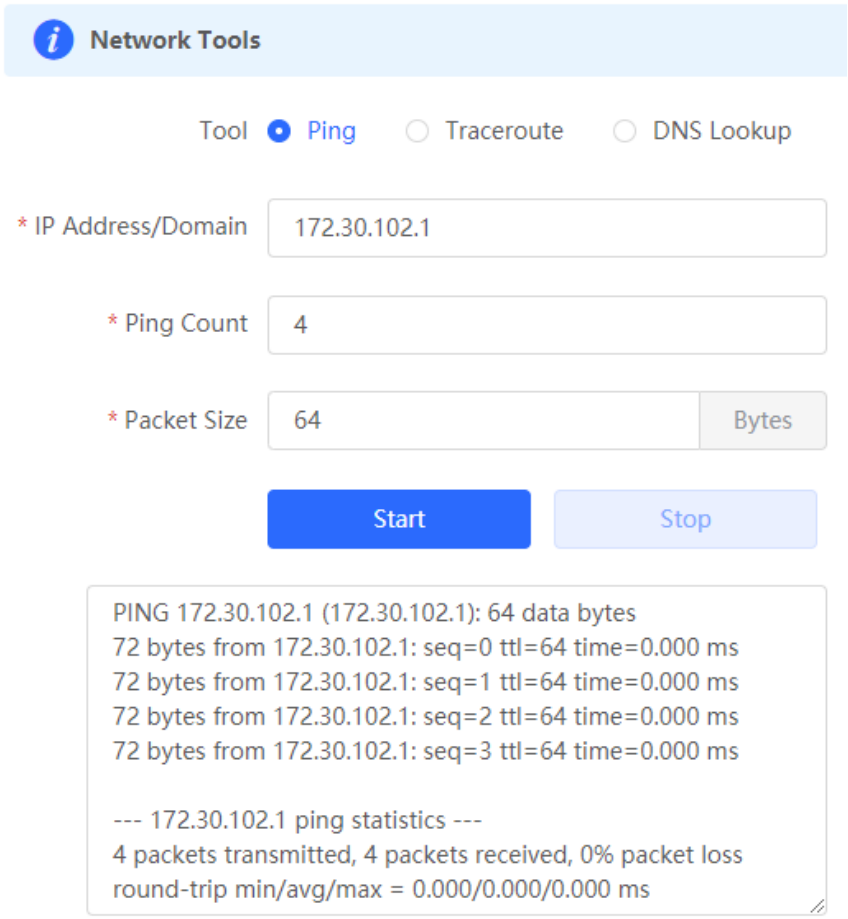
The **Network Tools** page provides three tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

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.

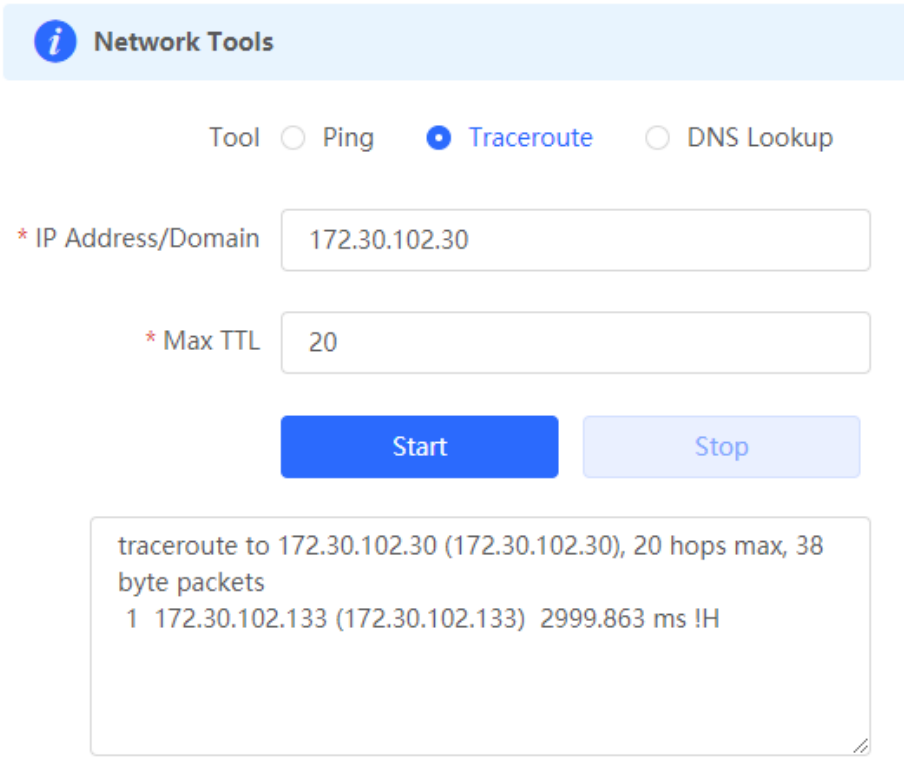


11.2.2 Traceroute

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**.

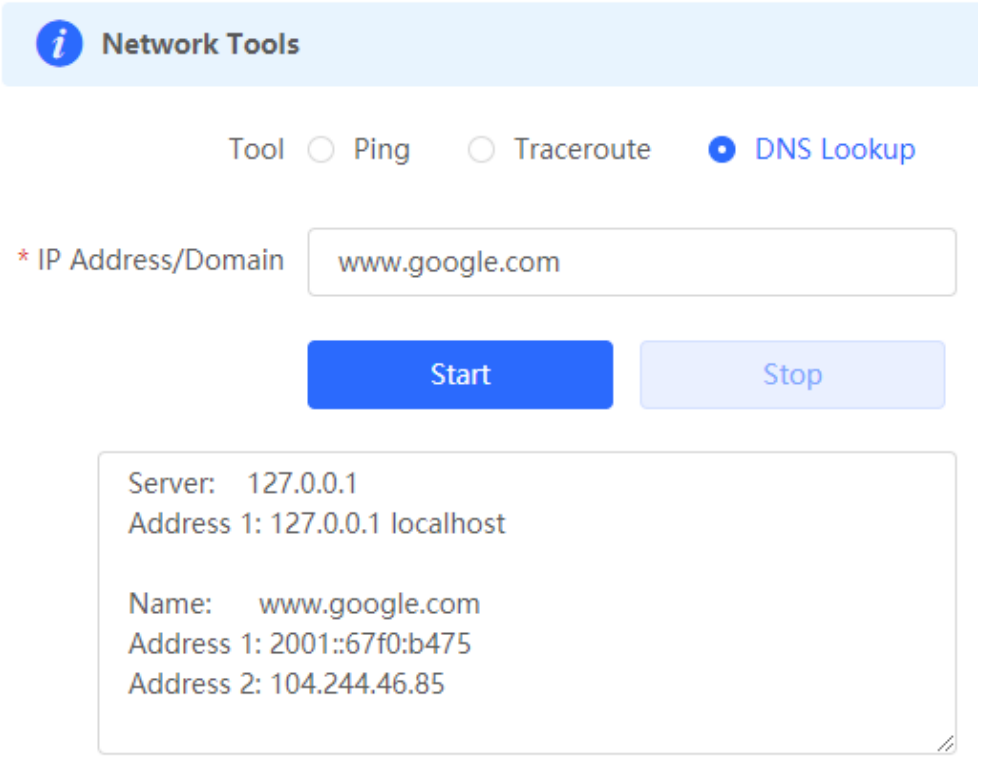


11.2.3 DNS Lookup

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.

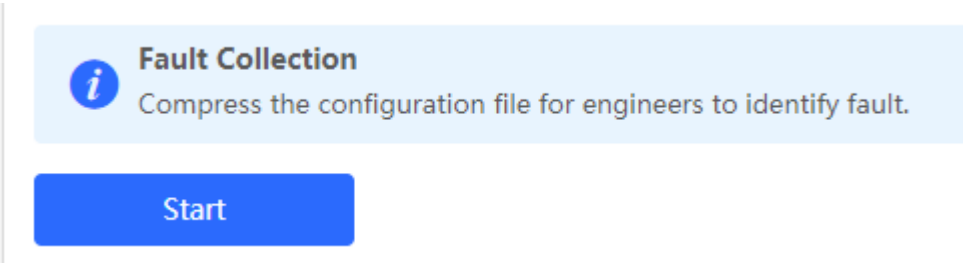
Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and click **Start**.



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.

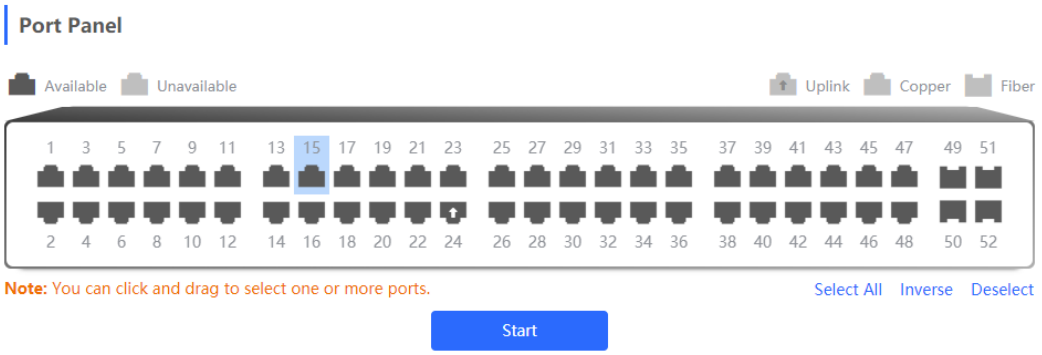


11.4 Cable Diagnostics

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.



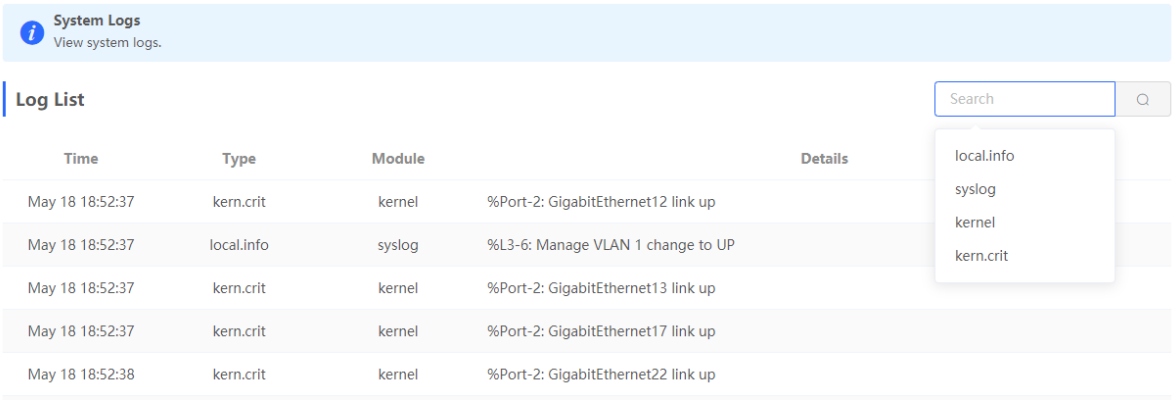
Caution

- 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.



11.6 Alerts

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

Note

Choose **Network** > **Alerts** to view the alert information of other devices in the network.

Displays possible problems on the network environment to facilitate fault prevention and troubleshooting. You can view the alert occurrence time, port, alert impact, and handling suggestions, and rectify device faults according to handling suggestions.

All types of alerts are concerned by default. You can click **Unfollow** to unfollow this type of alert. The system will no longer display this type of alert. To enable the notification function of a type of alert again, follow the alert type on the **Removed Alert** page.

Caution

After unfollowing an alert, the system will not issue an alert prompt for this type of fault, and users cannot find and deal with the fault in time. Exercise caution when performing this operation.

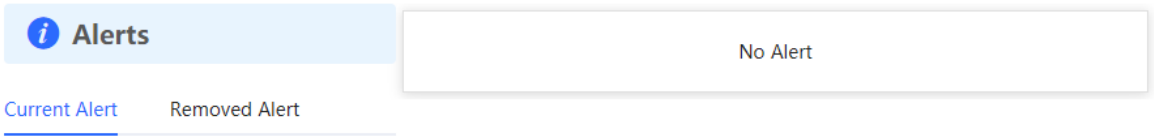


Table 11-1 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series, RG-NBS3200 Series Switches do not support this type of alert.

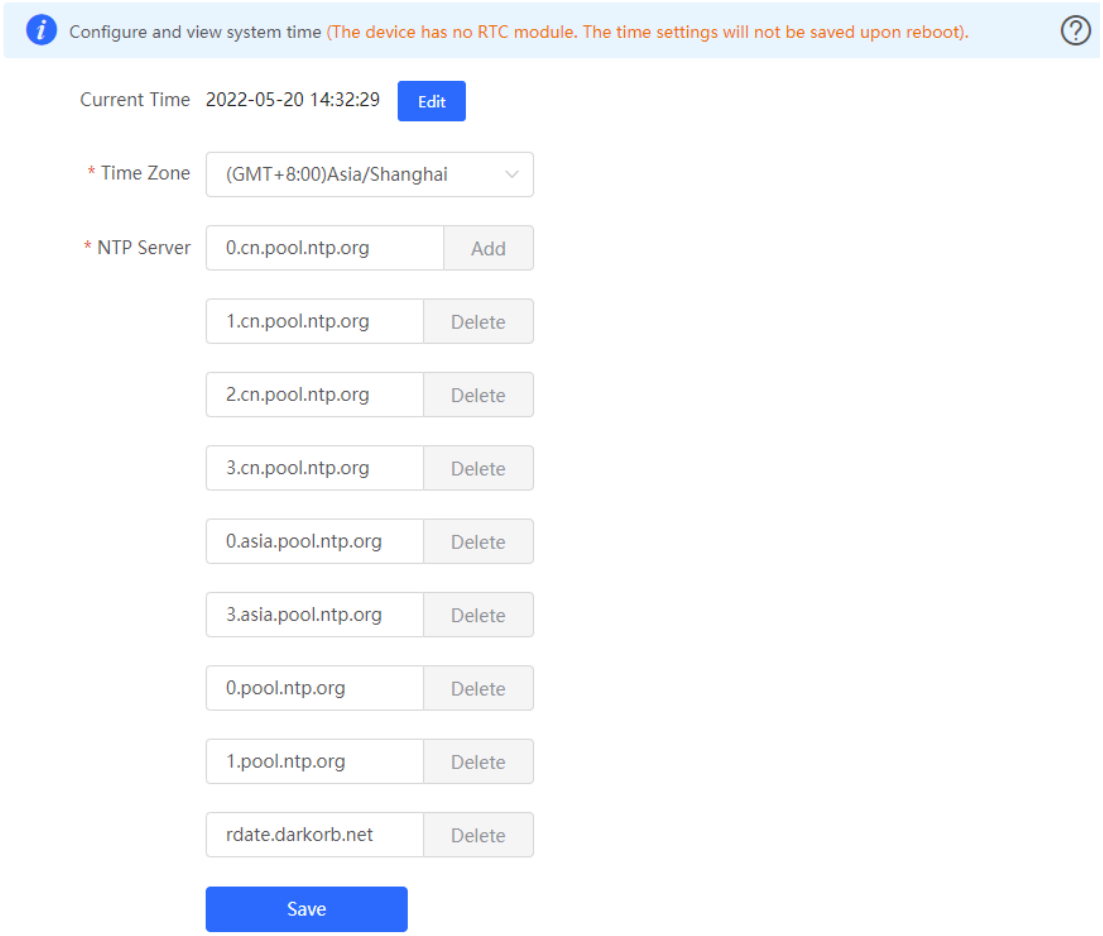
Alert Type	Description	Support Description
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	NA
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	NA
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of the product.	NA
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	NA
The PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and the new connected PD cannot be powered properly.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	NA

12 System Configuration

12.1 Setting the System Time

Choose **System** > **System Time**.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.



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

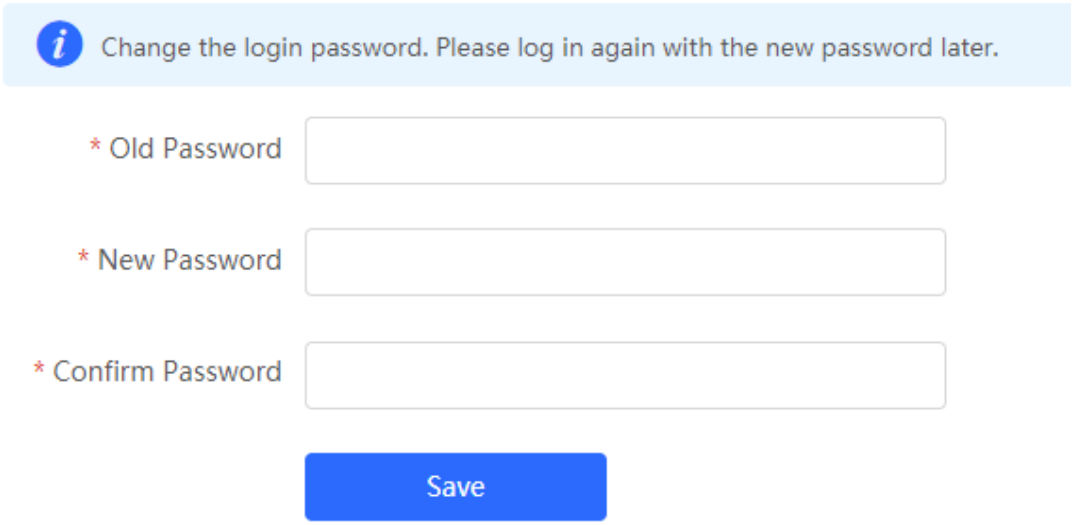
12.2 Setting the Web Login Password

Choose **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.



12.3 Setting the Session Timeout Duration

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

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

12.4 Configuring SNMP

12.4.1 Overview

SNMP (Simple Network Management Protocol) is a protocol used for managing network devices. It is based on the client/server model and can remotely monitor and control network devices.

SNMP consists of a management station and agents, with the management station communicating with agents through the SNMP protocol to obtain information such as device status, configuration information, performance data, etc., while also being able to configure and manage devices.

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

12.4.2 Global Configuration

1. Overview

The purpose of global configuration is to enable SNMP services and implement basic configurations such as SNMP protocol version (v1/v2c/v3), local port settings, device location settings, contact information settings.

SNMPv1: v1 is the earliest version of SNMP with poor security that only supports simple community string authentication. The v1 version has some defects such as plaintext transmission of community strings which makes it vulnerable to attacks; therefore it is not recommended for use in modern networks.

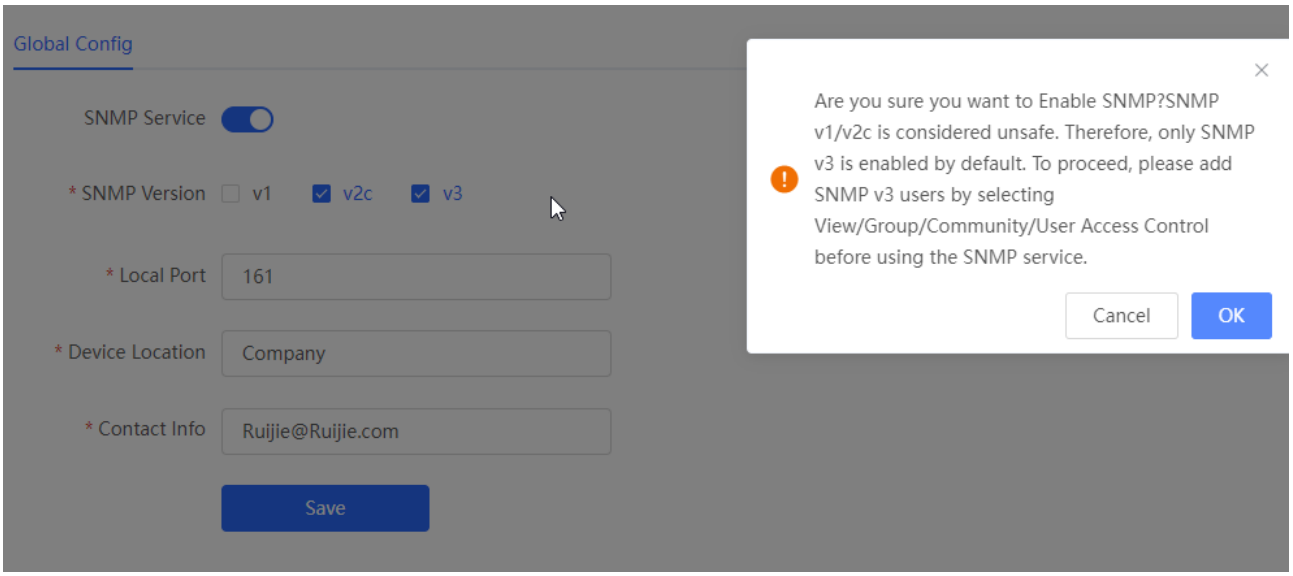
SNMPv2c: v2c is an improved version over v1 that supports richer functionality and more complex data types while enhancing security measures compared to its predecessor. The v2c version provides better security features than v1 along with greater flexibility allowing users to configure according to their specific needs.

SNMPv3: This latest version of the SNMP protocol includes additional security mechanisms like message authentication encryption compared to its predecessors - V1 & V2C - resulting in significant improvements in terms of access control & overall safety measures implemented by this standard.

2. Configuration Steps:

[Network-wide Management-Page Wizard] System >> SNMP>>Global Config

(1) Enable SNMP services.



When first opened, the system prompts to enable SNMPv3 by default. Click <OK>.

(1) Set global configuration parameters for SNMP service.

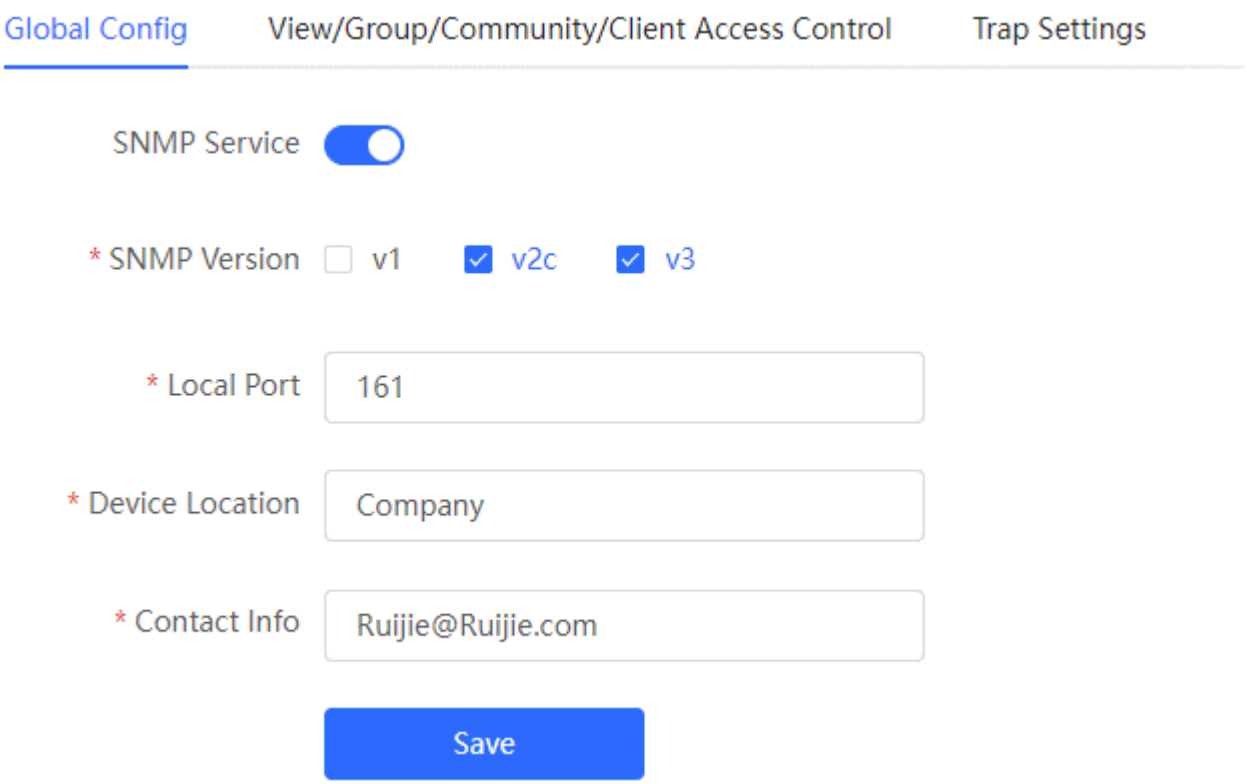


Table 4-1 **Global Configuration Description Table**

Parameter	Parameter
SNMP Service	Whether the SNMP service is enabled or not.

Parameter	Parameter
SNMP Protocol Version	SNMP protocol version number includes v1 version, v2c version, and v3 version.
Local Port	[1, 65535]
Device Location	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.
Contact Information	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.

(2) Click <Save>.

After enabling the SNMP service takes effect, click <Save> to make basic configurations such as SNMP protocol version number take effect.

12.4.3 View/Group/Community/Client Access Control

1. View/Group/Community/Client Access Control

MIB (Management Information Base) can be regarded as a database of different status information and performance data of network devices containing a large number of OID (Object Identifiers), which are used to identify different status information and performance data of network devices in snmp.

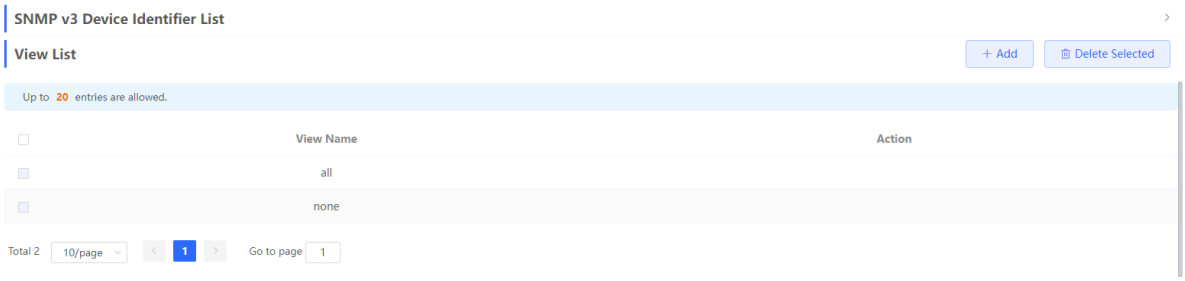
The role of views in snmp is to limit the node range that management systems can access in MIBs so as to improve network management security and reliability. Views are an indispensable part of SNMP management that needs to be configured and customized according to specific management requirements.

Views can define multiple subtrees according to requirements limiting the MIB nodes that management systems can only access within these subtrees while unauthorized MIB nodes cannot be accessed by unauthenticated system administrators thus protecting network device security. At the same time views also optimize network management efficiency improving response speed for managing systems.

Configuration Steps:

[Network-wide Management - Page Wizard] System >> SNMP >> View/Group/Community/Client Access Control >> View List

(1) Click <Add> to create a view.



(2) Configure the basic information of the view.

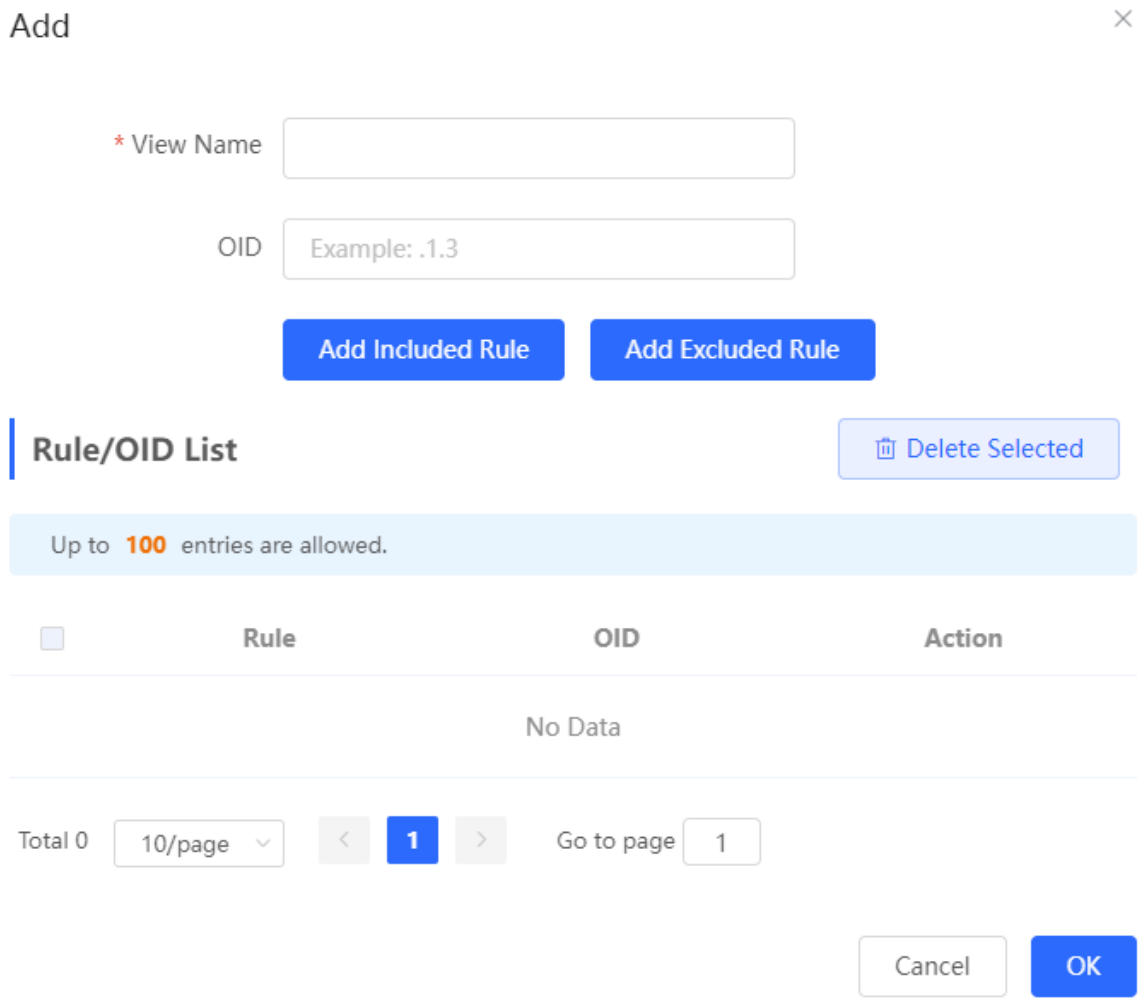


Table 4-1 **view information description table**

parameter	illustrate
View Name	The name used to identify the view. The length is 1 to 32 characters, and cannot contain Chinese and full-width characters.

parameter	illustrate
OIDs	Define the range of OIDs included in the view, which can be a single OID or a subtree of OIDs
Add Included Rule or Excluded Rule Add Included Rule Add Excluded Rule	Divided into inclusion rules and exclusion rules ● Include rules allow access only to OIDs within the OID range . Click <Add Inclusion Rule> to set up this type of view. ● Exclusion rules allow access to all OIDs except the OID range . Click <Add Exclusion Rule> to set up this type of view.

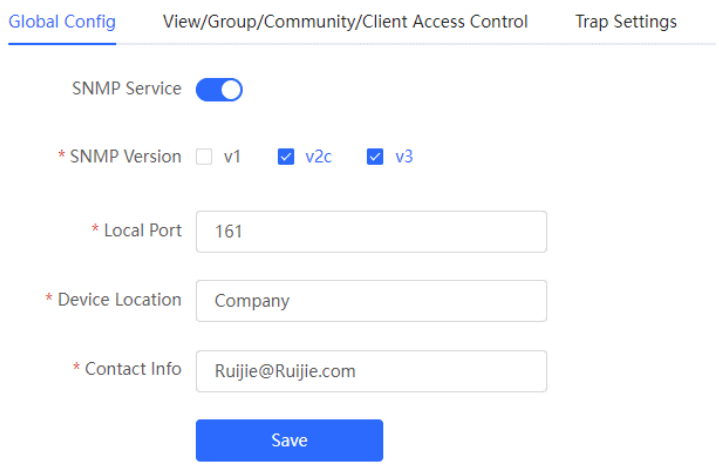
Notice

For the created view, add at least one OID rule , otherwise a warning message will appear .

(2) Click <OK> .

2. v1 /v2c user configuration

- Introduction
- When the SNMP protocol version is set to v1/v2c, user configuration needs to be completed.



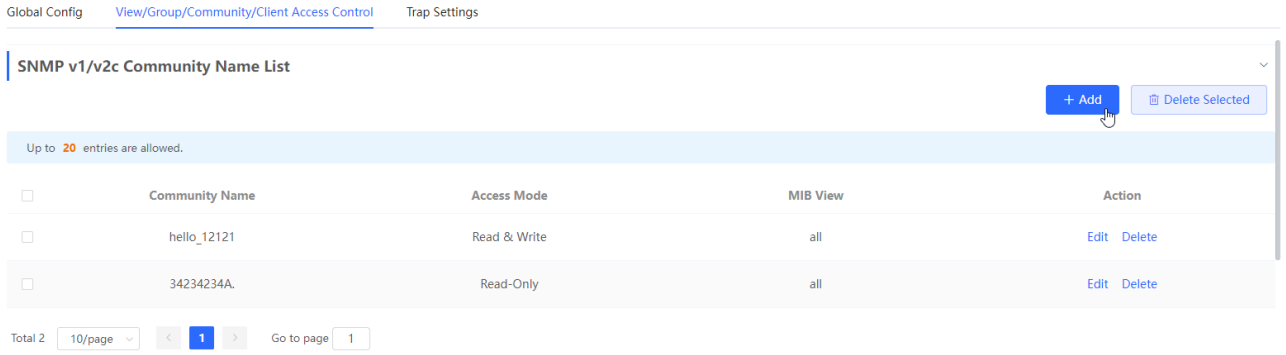
instruction

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

[Entire Network Management-Page Wizard] System>>SNMP>> View/Group/Community/Client Access Control

(1) In the " SNMP v1/v2c Community Name List " area, click <Add>.



(2) Create v1/v2c users.

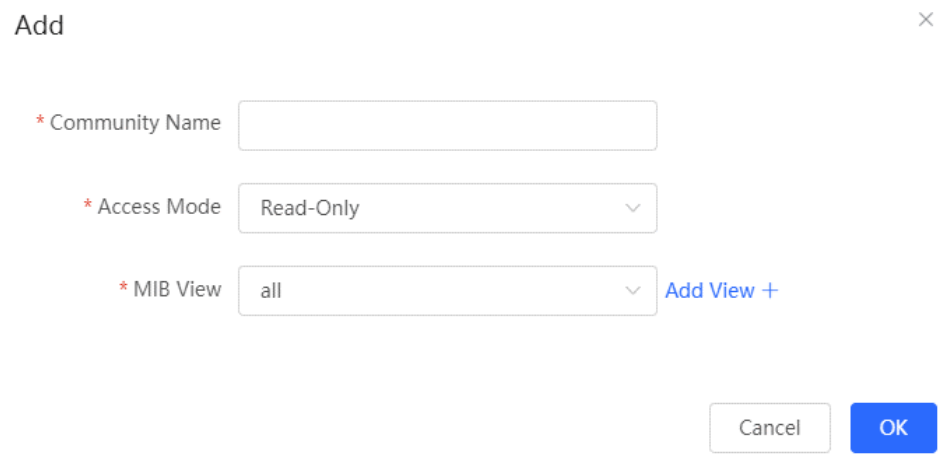


Table 4-1 **v1 / v2c user information description table**

parameter	**illustrate**
Community Name	at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private

parameter	illustrate
	Do not contain question marks, spaces and Chinese
Access Mode	Access rights of the community name (read-only , read-write) Read & Write Read-Only
MIB View	The options in the drop-down box are configured views (default views all , none)

Notice

- Among v1/v2c users, the community name cannot be repeated .
- Click <Add View> to add a view .

3. v3 group configuration

- Introduction

SNMPv3 introduces the concept of grouping for better security and access control. A group is a group of SNMP users with the same security policy and access control settings. Using SNMPv3 , multiple groups can be configured, each group can have its own security policy and access control settings, and each group can also have one or more users.

- prerequisite

When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.

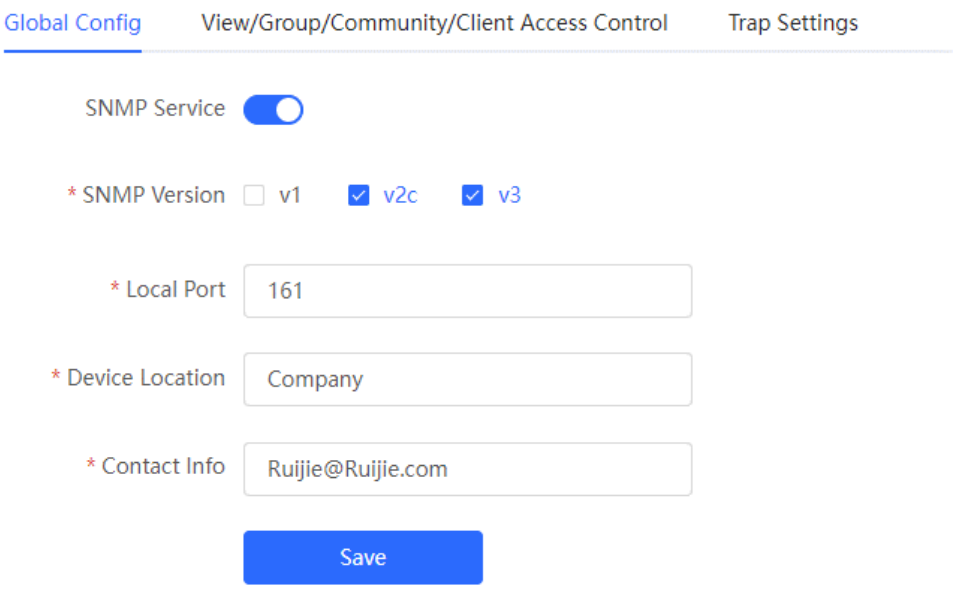
illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control.

(1) Click <Add> in the " SNMP v3 Group List " area to create a v3 group .



(2) Set v 3 groups of related parameters.

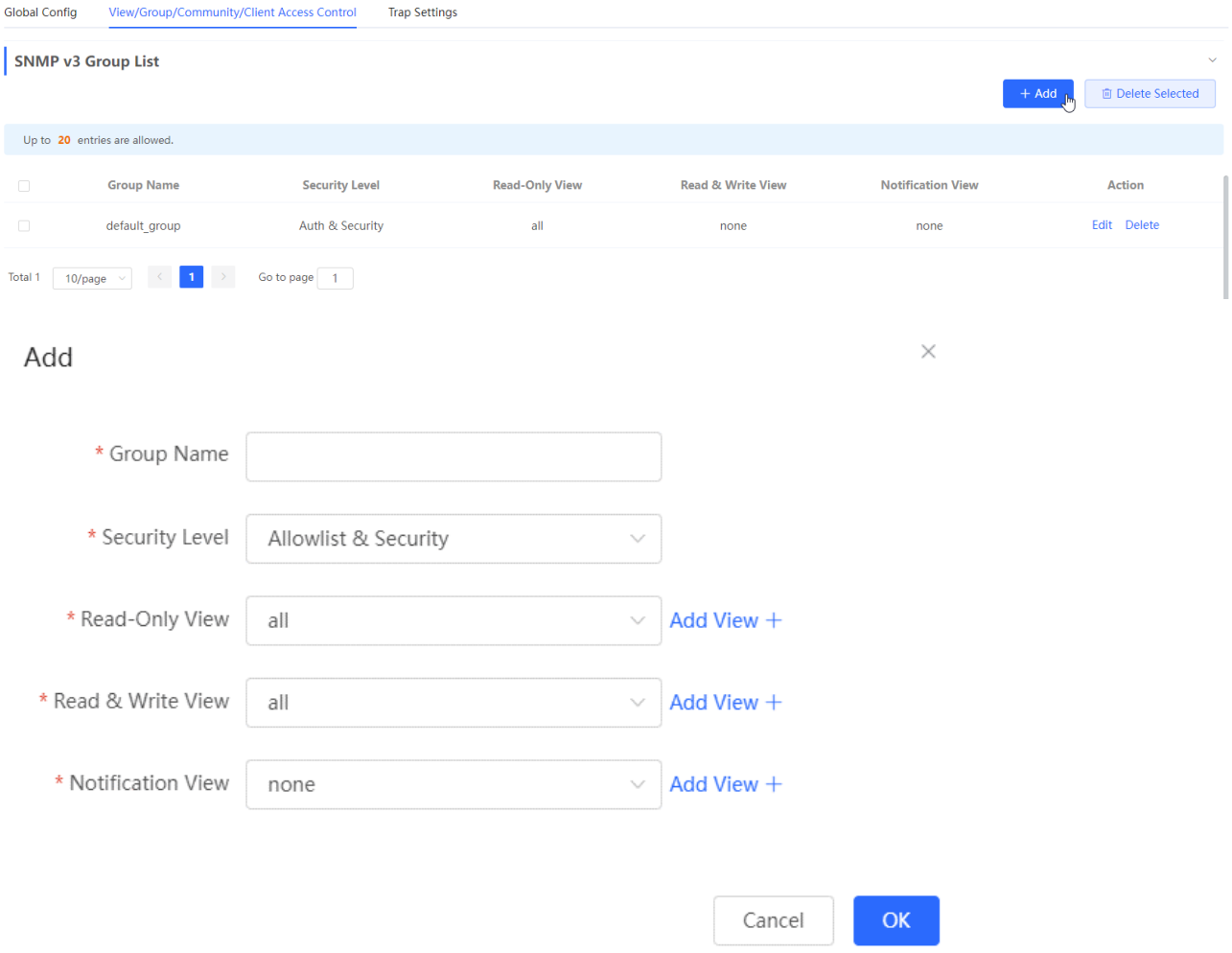


Table 4-1 **V3 group configuration parameters**

parameter	illustrate
Group Name	rule group name 1-32 characters, a single Chinese accounted for three characters Cannot contain Chinese, full-width characters, question marks and spaces
Security Level	The minimum security level of the rule group (**Auth & Security** Auth & Open Allowlist & Security authentication with encryption, authentication without encryption, no authentication encryption)
Read-Only View	The options in the drop-down box are configured views (default views all , none)
Read & Write View	The options in the drop-down box are configured views (default views all , none)
Notification View	The options in the drop-down box are configured views (default views all , none)

⚠ Notice

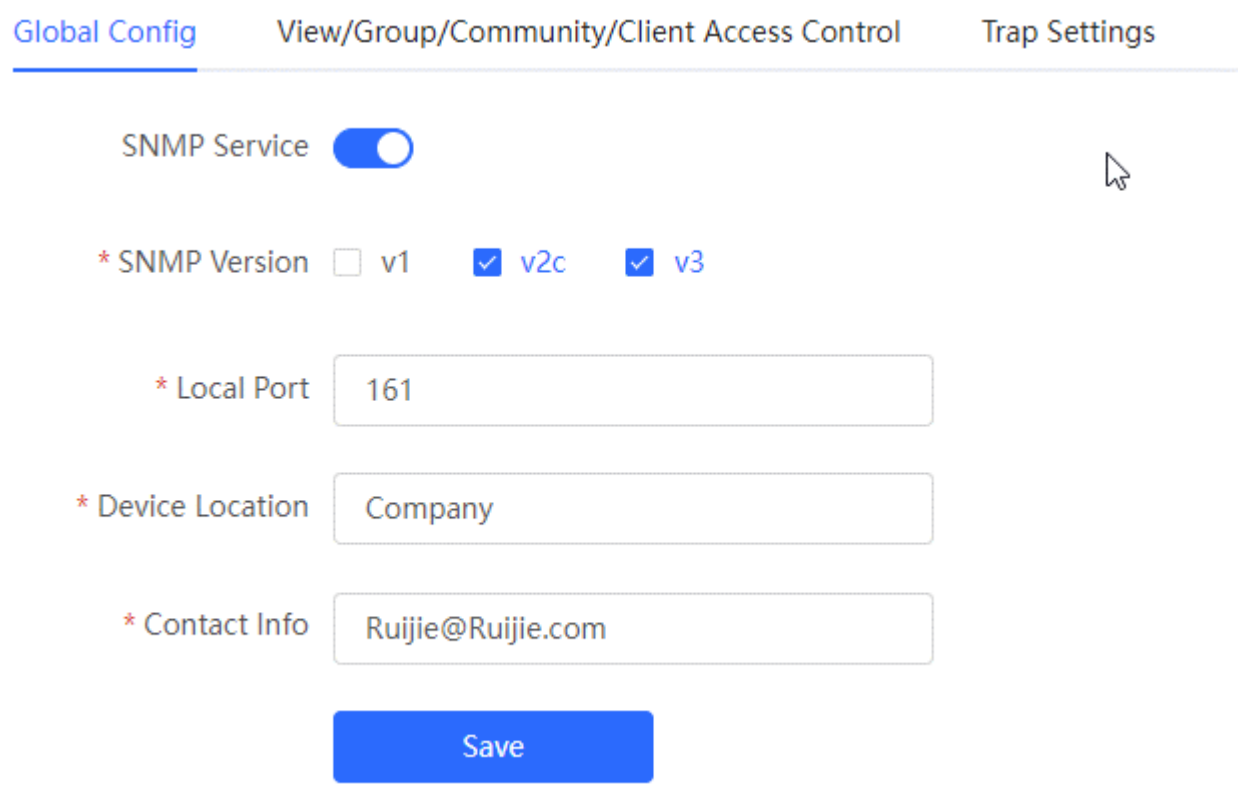
- Groups limit the minimum security level, read and write permissions and scope of users in the group.
- The group name cannot be repeated . If you need to add a view, click < Add View >.

(3) Click <OK> .

4. v 3 user configuration

- Introduction
- prerequisite

When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.



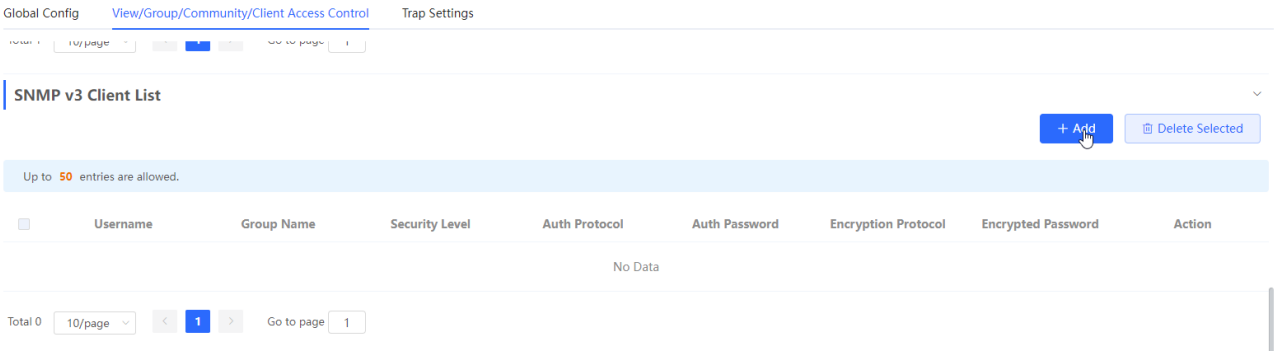
illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control >>.

(1) In the " SNMP v3 Client List " area, click <Add> to create a v3 user .



(2) Set v3 user related parameters.

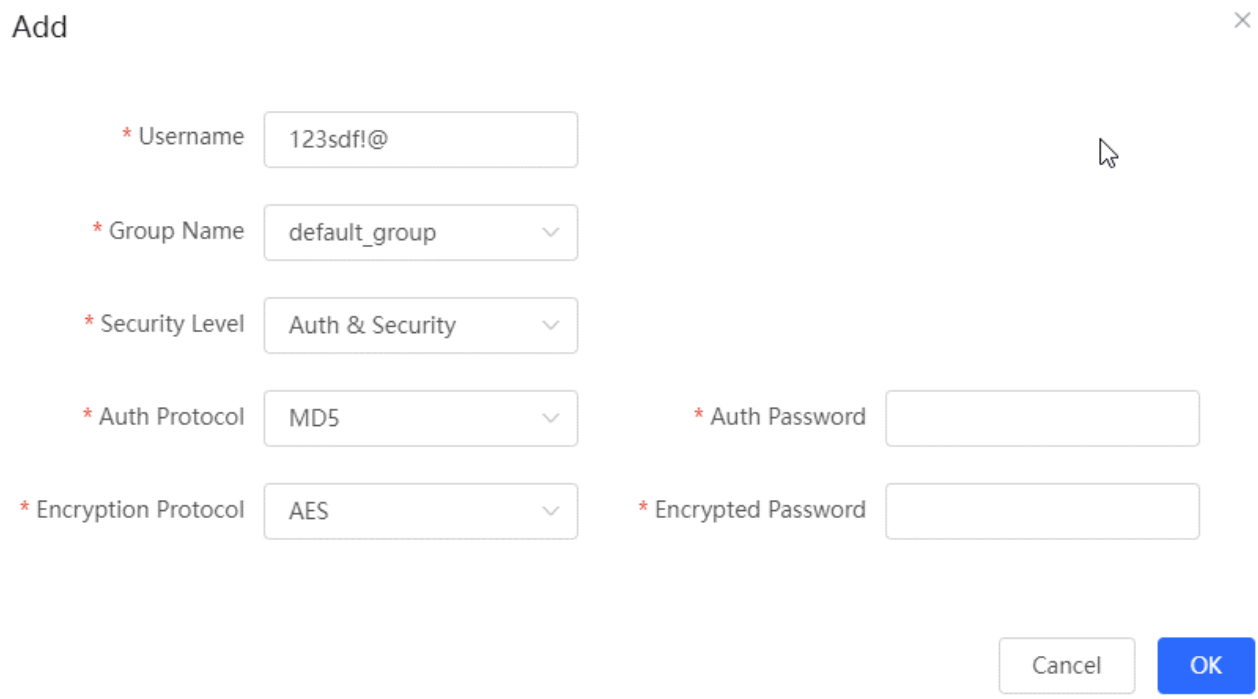


Table 4-1 **v3 user configuration parameters**

parameter	**illustrate**
Username	username at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Group Name	user's group
Security Level	User security level (authentication and encryption, authentication without encryption, no authentication and encryption)
Auth Protocol , Auth Password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces , and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters . Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".

parameter	illustrate
Encryption Protocol , Encrypted Password	Encryption protocols include: DES/AES/AES192/AES256 Encrypted password: the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format, containing at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.

⚠ Notice

- The security level of the v3 user must be greater than or equal to the security level of this group.
- There are three security levels. For authentication and encryption, you need to configure the authentication protocol, authentication password, encryption protocol, and encryption password. For authentication without encryption, you only need to configure the authentication protocol and encryption protocol. Without authentication and encryption, no configuration is required.

12.4.4 Typical Configuration Examples of SNMP Service

1. v2c version SNMP service configuration

- scenes to be used

The user only needs to monitor the information of the device, and does not need to set and send it. The data information of nodes such as 1.3.6.1.2.1.1 is monitored through the third-party software using the v2c version.

- configuration list

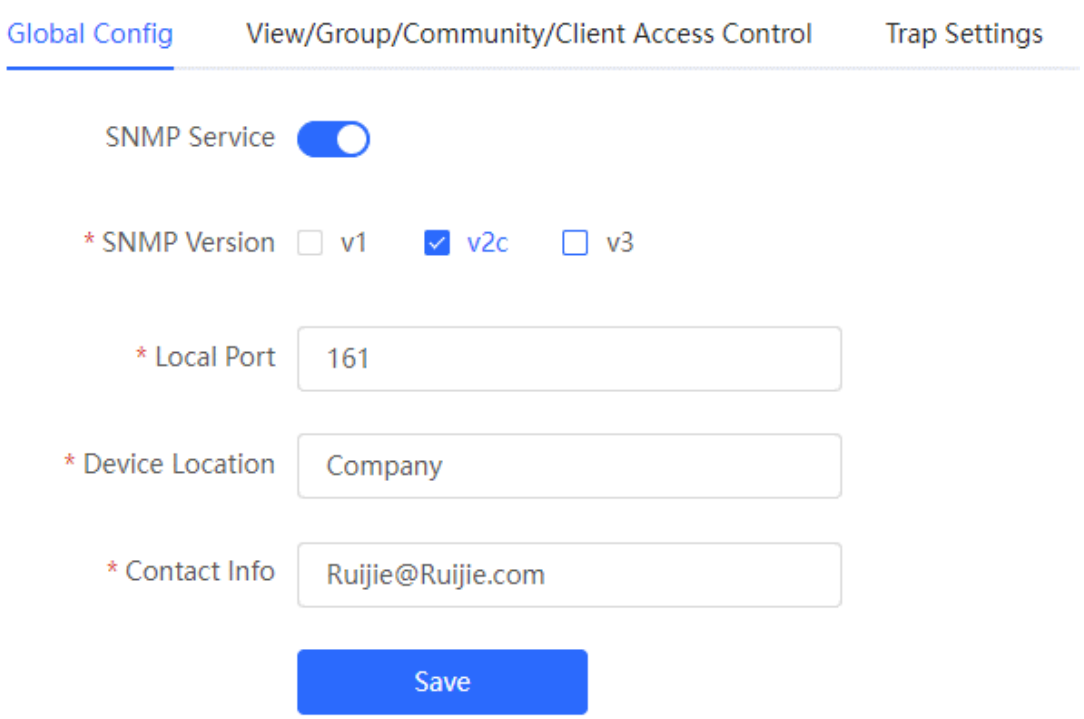
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

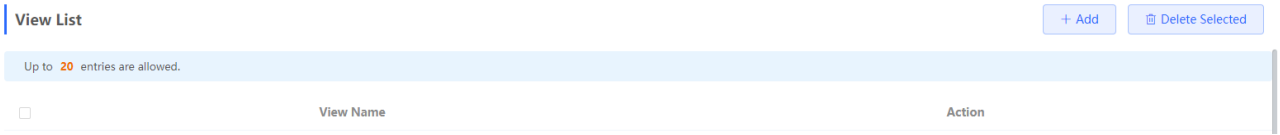
description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1.1 , custom view named " system "
use version number	v2c version The custom community name is " public ", and the default port number is 161
Read and write permissions	Read permission

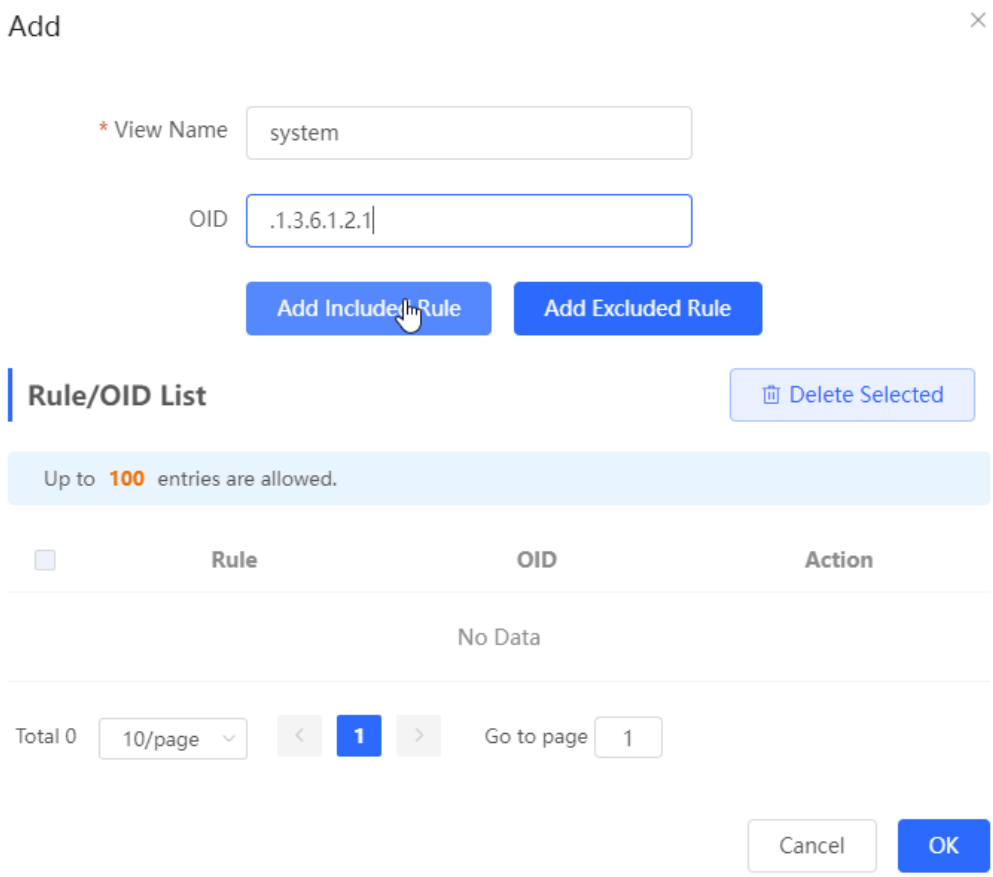
- configuration steps

(1) On the global configuration interface, select the v2c version, and leave other settings as default. After the operation is complete, click <Save> .

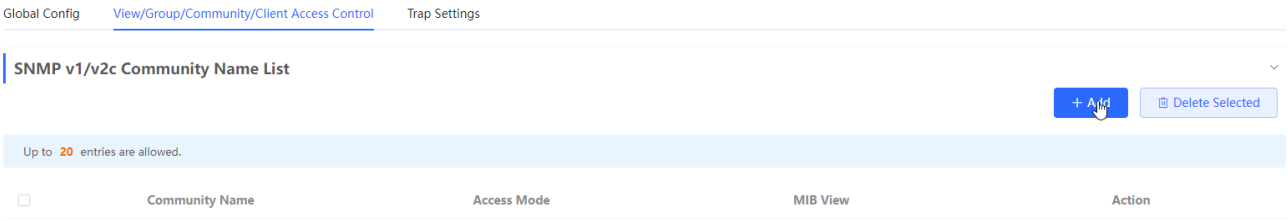


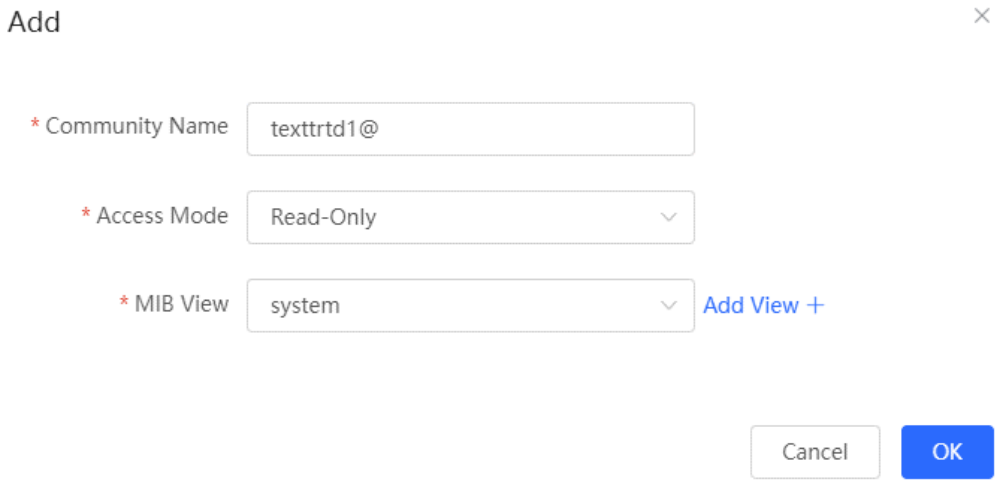
(2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and O ID in the pop-up window and click <Add inclusion rule>, and click <OK> after the operation is complete .





(3) view /group/group/user access control interface, 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.





2. v 3 version SNMP service configuration

- scenes to be used

Users need to monitor and control the equipment, and use the v3 version of the third-party software to monitor and send data to the public node (1.3.6.1.2.1) node. The security level of the v3 version adopts authentication and encryption.

- configuration list

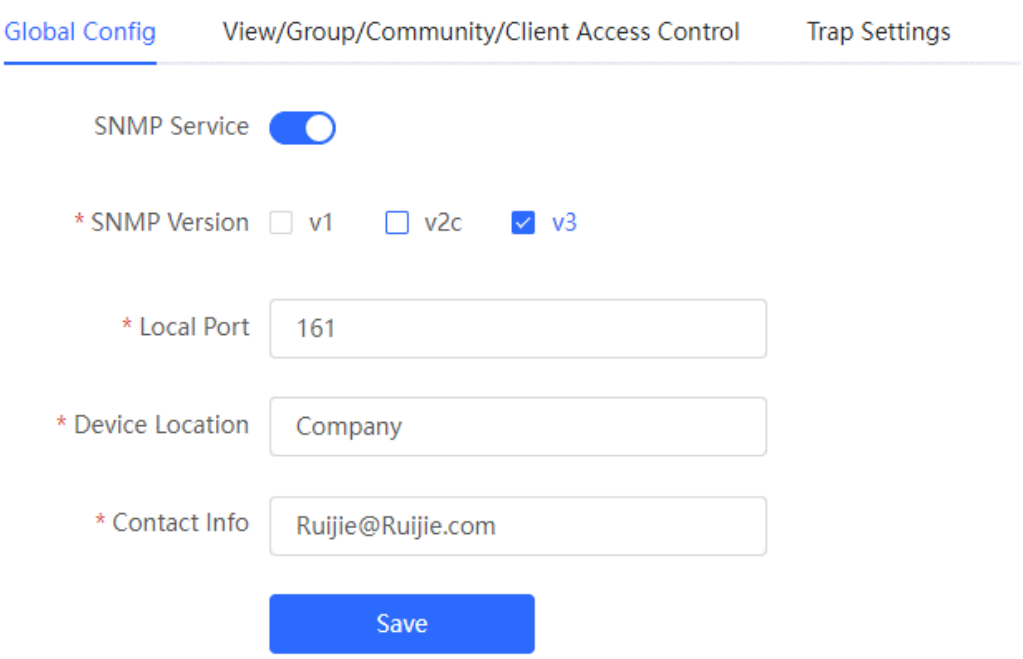
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

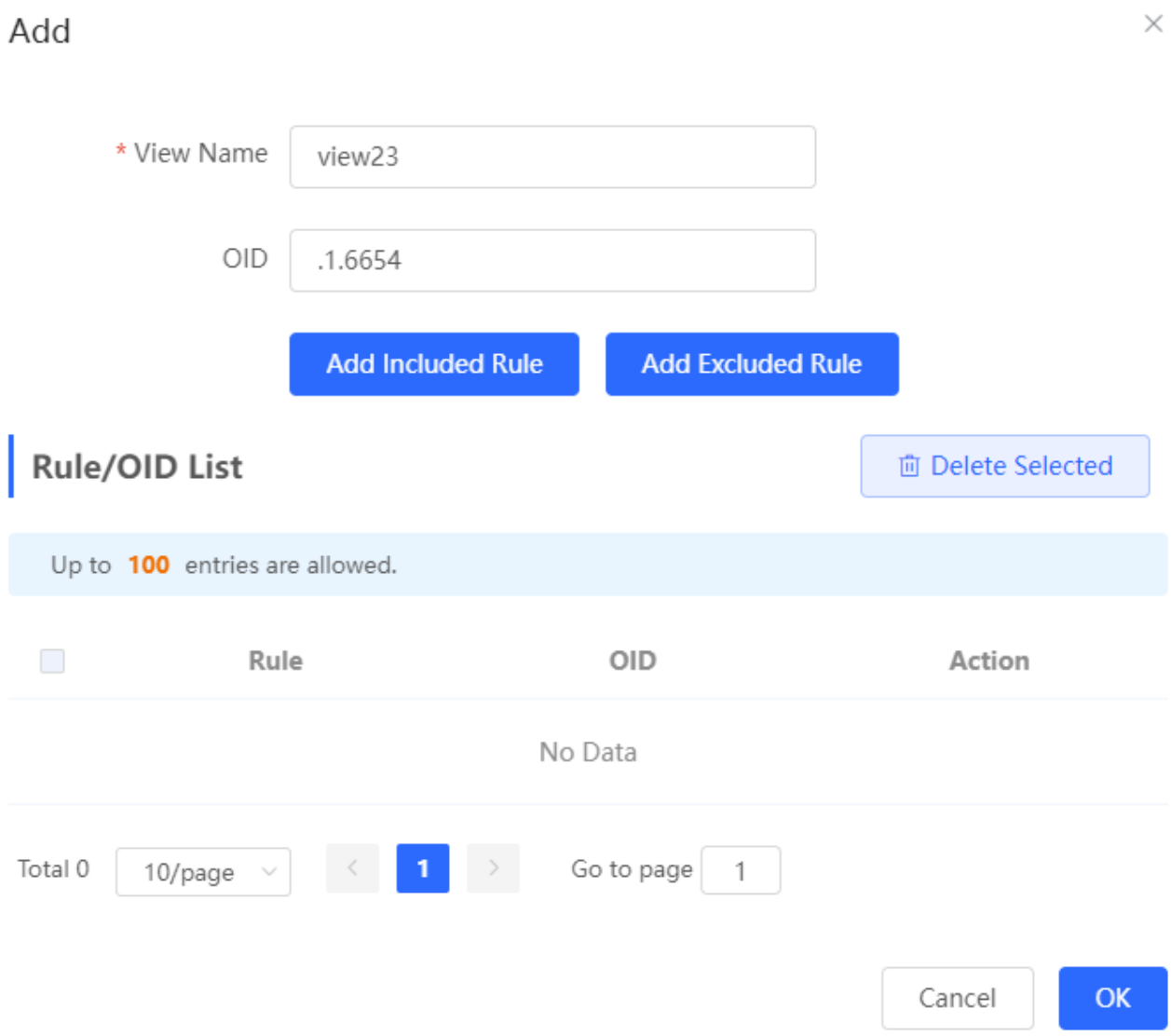
description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1 and custom view is named " public_view "
group configuration	Group name: group Security level: authenticated and encrypted Readable view select " public_view " Writable view select " public_view " Notification view select " none "
v3 user configuration	Username: v3_user Group name: group Security level: authenticated and encrypted Authentication protocol / authentication password: MD5/Ruijie123 Encryption protocol / encryption password: AES/ Ruijie123
use version number	v3 version, default port 161

- configuration steps

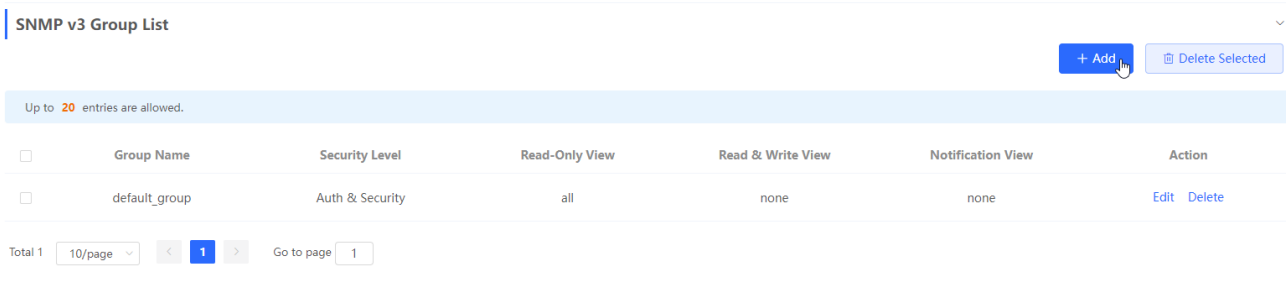
(2) Select the v3 version on the global configuration interface , change the port to 161, and set other settings to default. After the operation is complete, click <Save>.

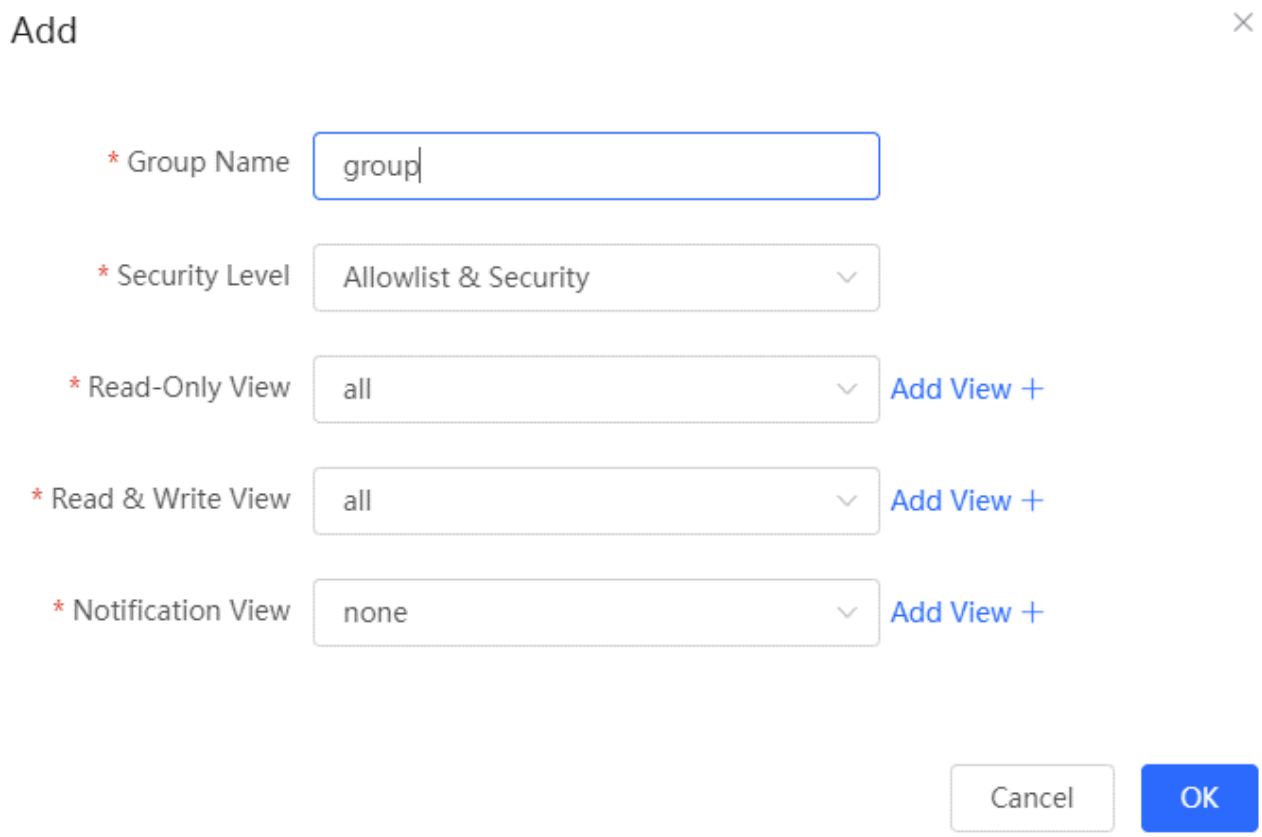


(2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and OID in the pop-up window, click <Add Inclusion Rule>, and click <OK> after the operation is complete.

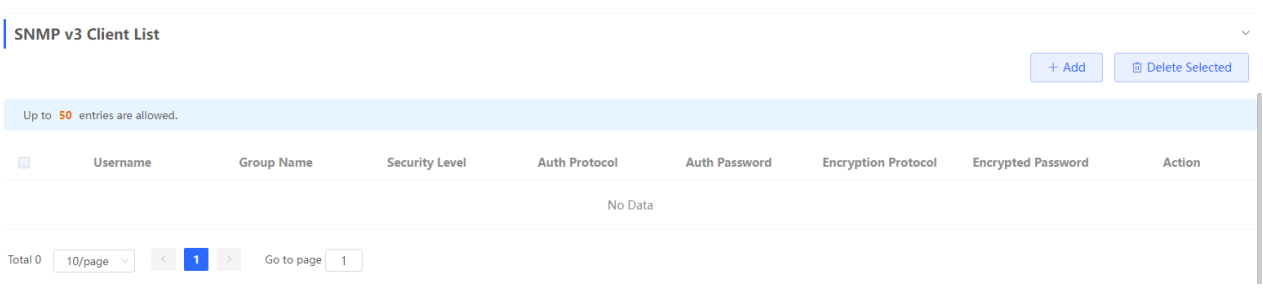


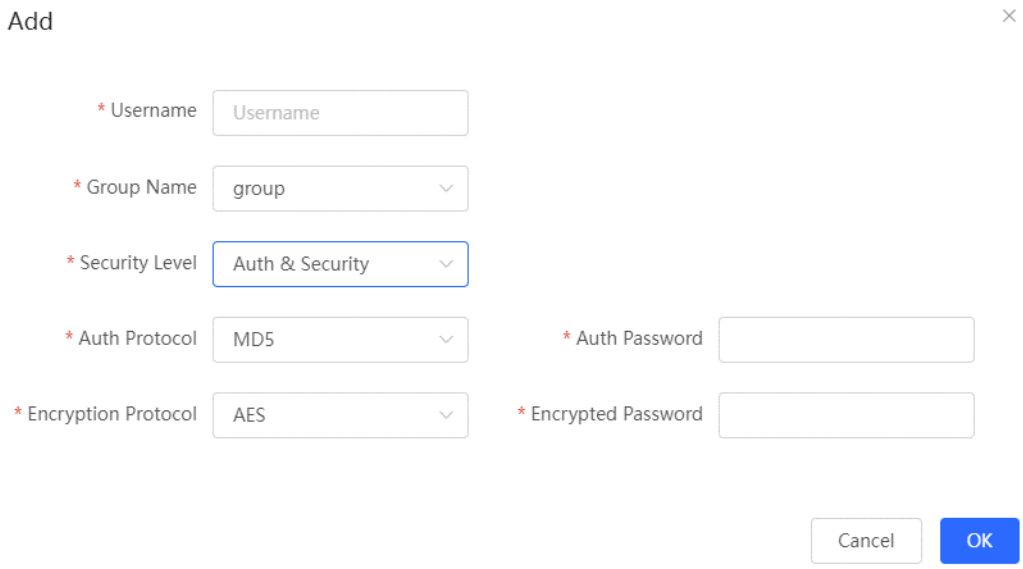
(3) Click <Add> in the SNMP v3 group list, fill in the group name and security level in the pop-up window, the user has read and write permissions, select "public _view" for the readable view and read and write view, and set the notification view to none , click < OK>.





(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>.





12.4.5 trap service configuration

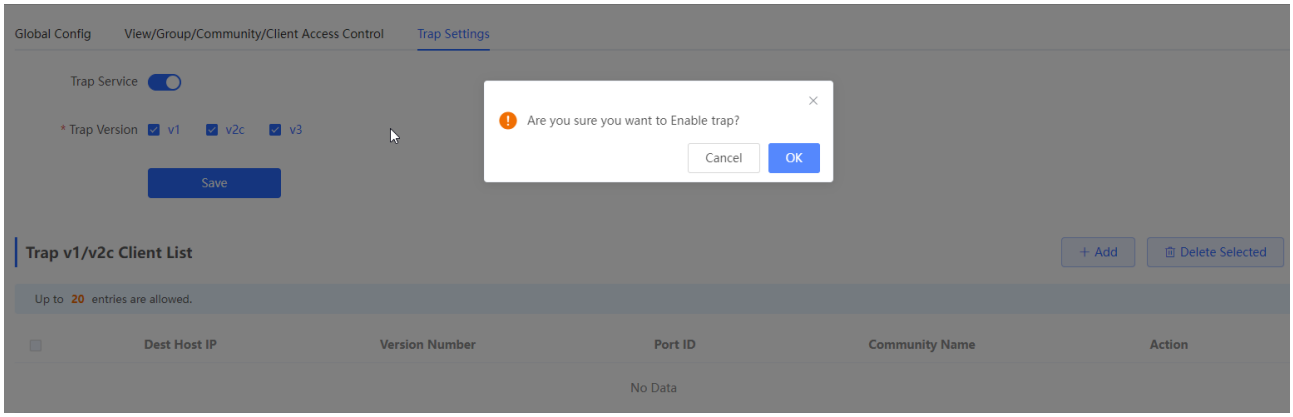
trap is a notification mechanism of SNMP (Simple Network Management Protocol) protocol, which is used to report the status and events of network devices to managers, including device status reports, fault reports, performance reports, configuration reports and security management. Trap can provide real-time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

1. trap open settings

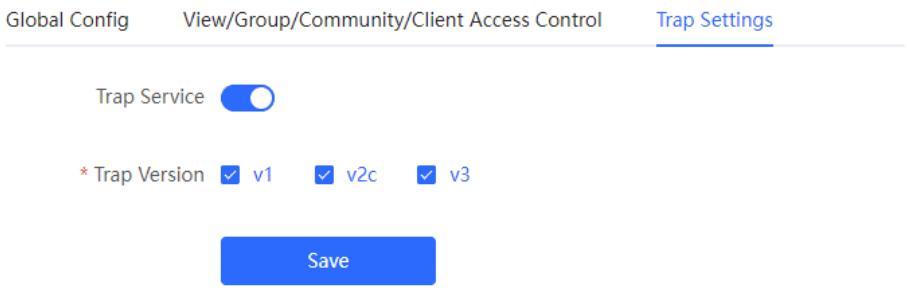
Enable the trap service and select the effective trap protocol version, including v1, v2c , and v3 .

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

(1) Enable the trap service switch.



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



(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 in the network in time and take corresponding measures.

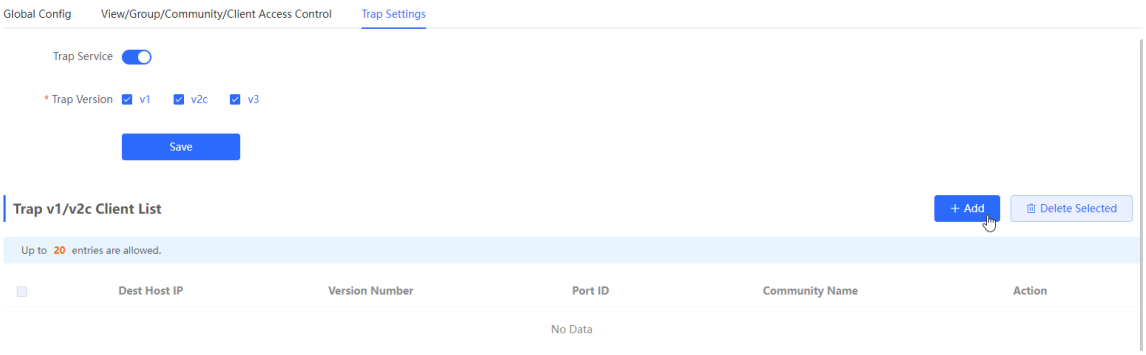
- prerequisite

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

- configuration operation

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

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



(2) Configure trap v1v2c user-related parameters.

set up

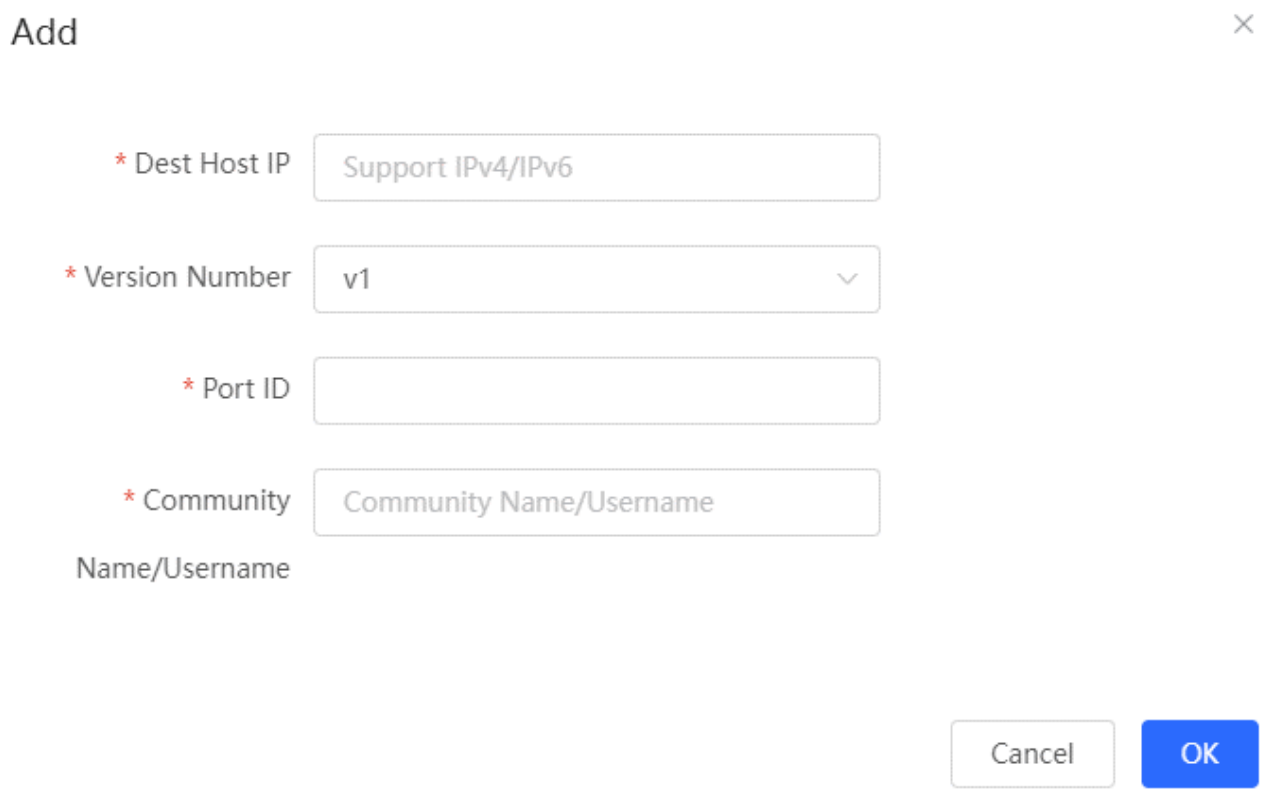


Table 4-1 **t rap v1/v2c user information description table**

parameter	**illustrate**
destination ip	Trap peer device IP, support IPv4 / IPv6 address
version number	Trap version number, including v1|v2c
The port number	trap peer device port [1, 65535]
Group Name/User Name	The community name of the trap user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese

Notice

- IP address of trap v1/v2c /v3 users cannot be repeated .
- Trap v1/v2c user names cannot be repeated.

(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.

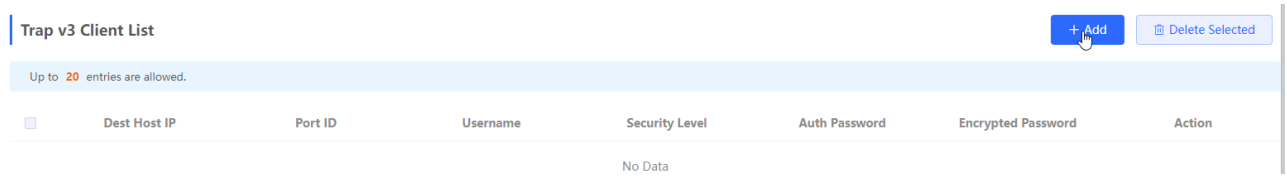
- prerequisite

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

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

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



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

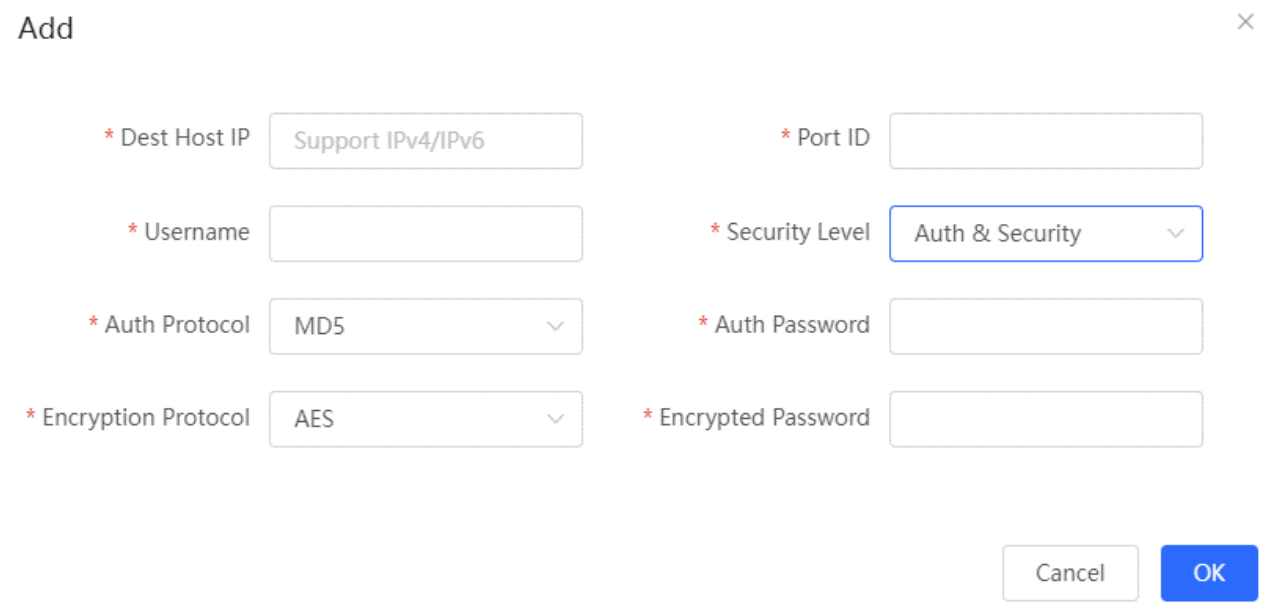


Table 4-1 **trap v3 user information description table**

parameter	illustrate
target host ip	trap peer device IP , support IPv4/IPv6 address
The port number	trap peer device port [1, 65535]
username	username of the trap v3 user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Security Level	Trap user security level, including three levels of authentication and encryption, authentication and encryption, and authentication and no encryption
Authentication protocol, authentication password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~ 31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces, and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".
encryption protocol, encryption password	Encryption protocols include: DES/AES/AES192/AES256 Encrypted password: the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format, containing at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.

⚠ Notice

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

- scenes to be used

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 list

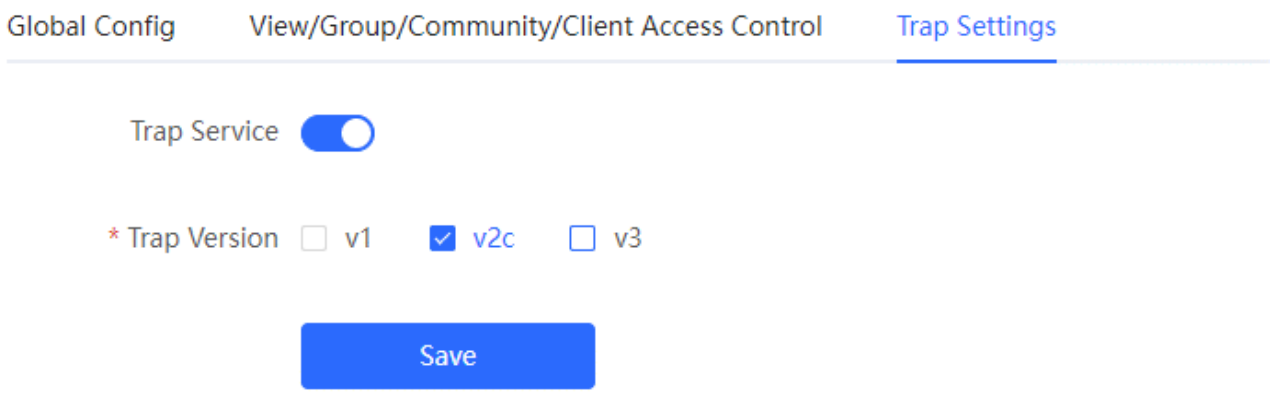
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

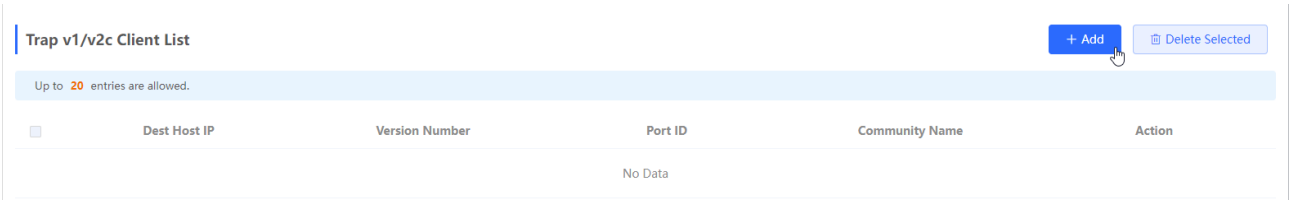
description item	illustrate
IP and port number	The target host IP is "192.168.110.85" , and the port number is "166" .
use version number	Select v2 version
Group Name / User Name	Trap_public

- configuration steps

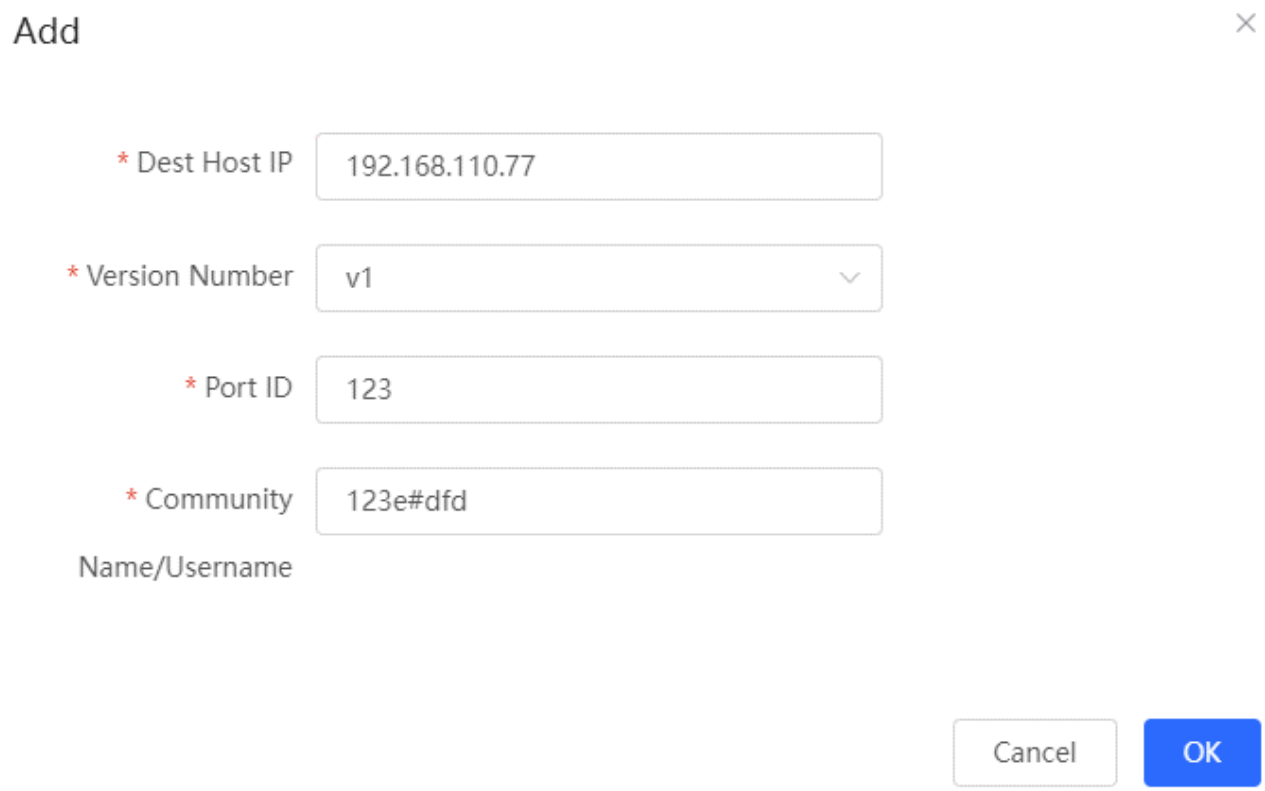
(3) Select the v2c version on the trap setting interface , click <Save> ,



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



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



2. V3 version trap configuration

- scenes to be used

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 68.110.87 and the port number 1 67 , and use the more secure v3 version to send traps.

- configuration list

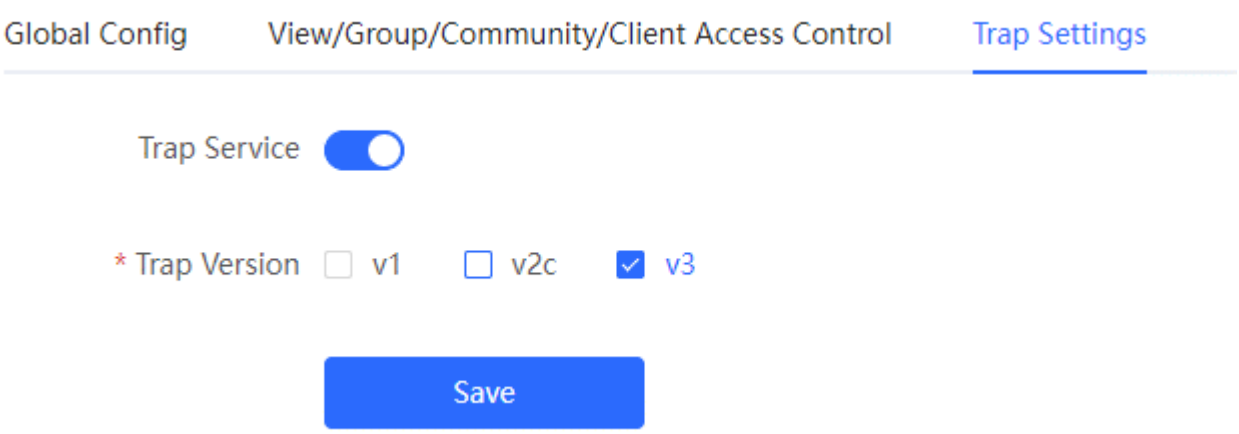
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

description item	illustrate
IP and port number	The target host IP is "192.168.110.87" , and the port number is "167" .
Use version number, username	Select the v3 version, the user name is "trapv3_public"
Authentication Protocol / Encryption Protocol Encryption Protocol / Encryption Cipher	Authentication protocol / authentication password: MD5/Ruijie123 Encryption protocol / encryption password: AES/ Ruijie123

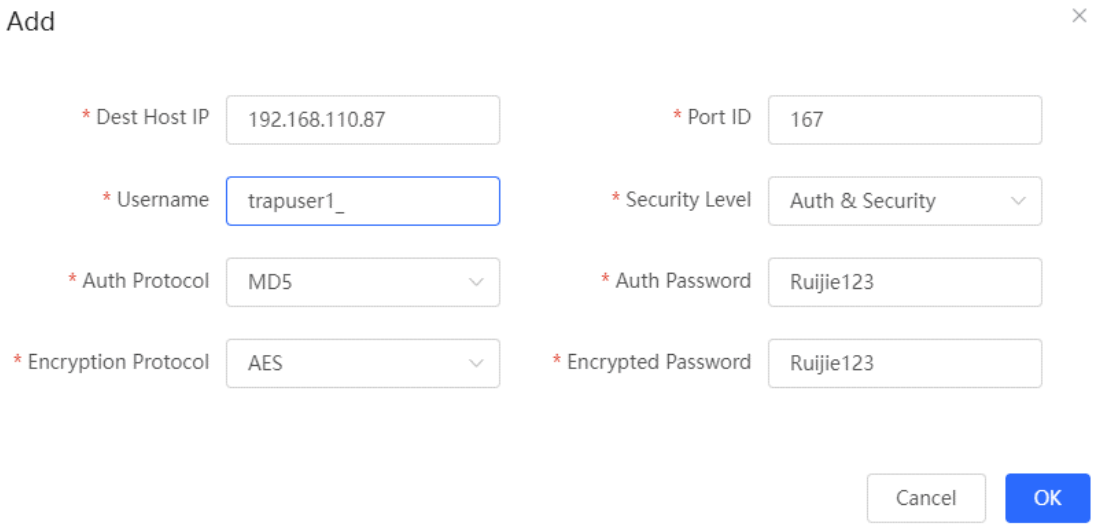
- configuration steps

(4) Select the v3 version on the trap setting interface , and click <Save> .



(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.



12.5 Configure 802.1x authentication

12.5.1 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 .

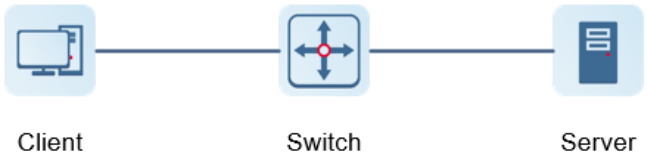
- Authentication : Authentication, used to determine whether users can obtain access rights and restrict illegal users;
- Authorization : Authorization, which services authorized users can use, and control the rights of legitimate

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.

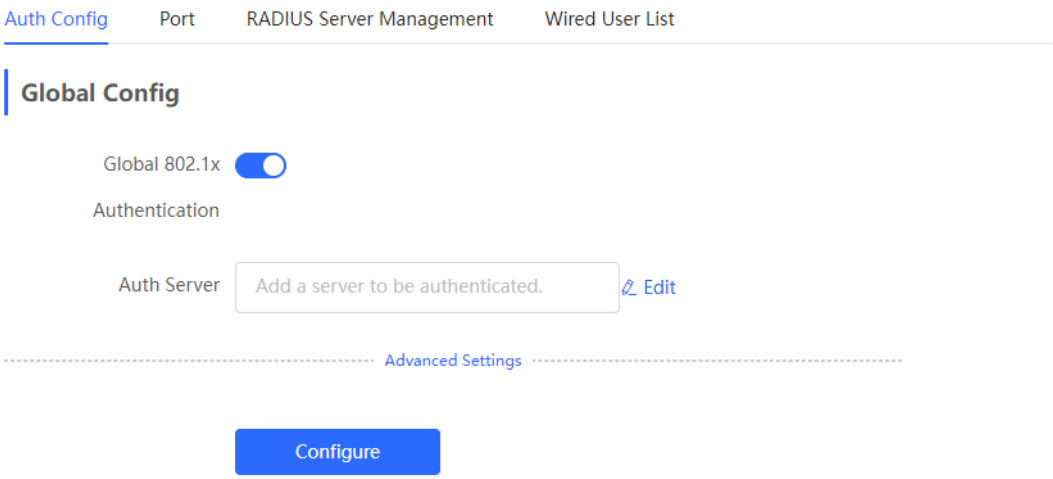
illustrate

RG- NBS switching devices only support the authentication function.

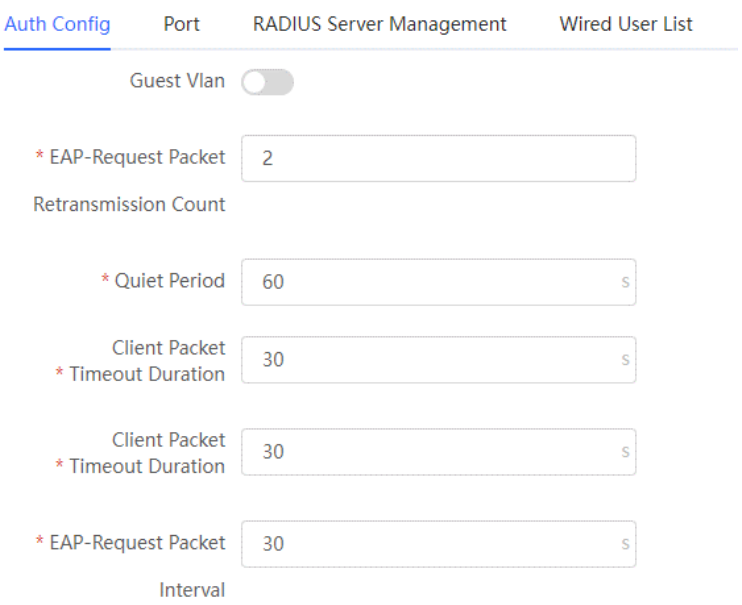
12.5.2 Configuration 802.1x

[Local Management - Page Wizard] Security > 802.1x Authentication > Auth _ Config

(1) Click the " Global 802.1x " switch, the system prompts to confirm whether to enable it, click <Configure>.



Click Advanced Settings to configure parameters such as Guest VLAN .

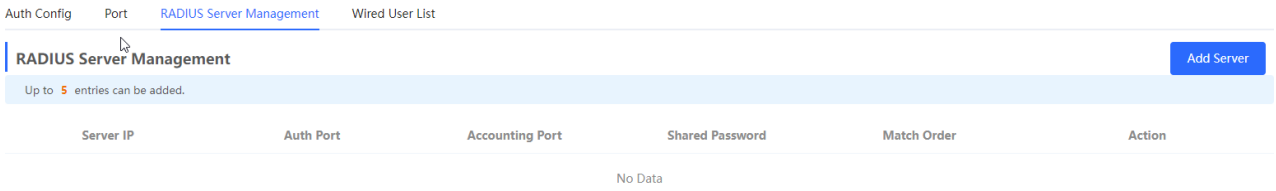


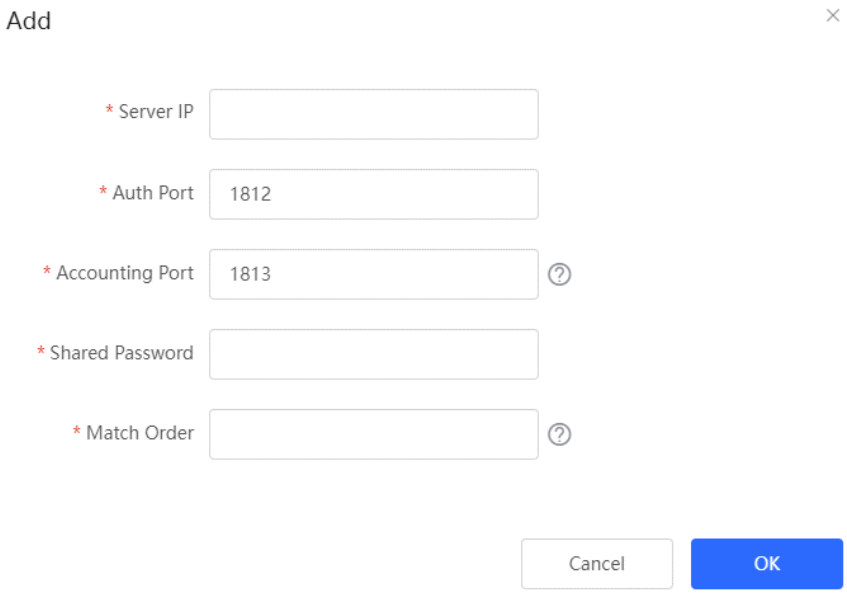
parameter	illustrate
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
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 considered 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

(2) 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 .

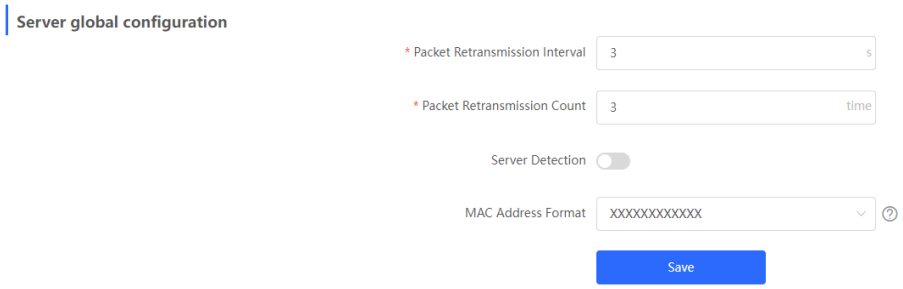




parameter	Reference without translation	illustrate
Server IP	server address	Radius server address.
Auth Port	authentication port	The port number used for accessing user authentication on the Radius server.

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

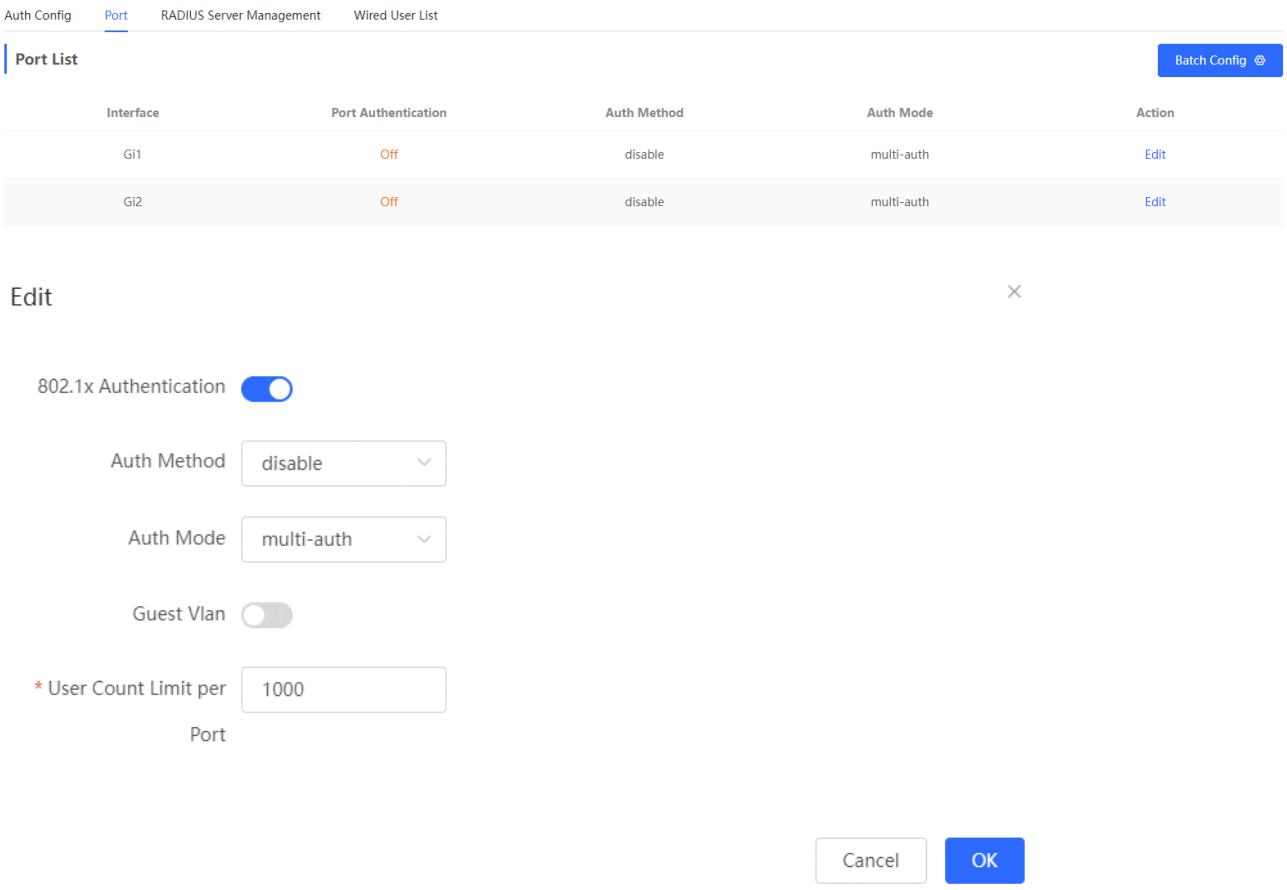
(1) Set up the server and click <Save> .



parameter	reference - do not translate	illustrate
Packet Retransmission Interval	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	Packet retransmission times	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
Server Detection	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.

parameter	reference - do not translate	illustrate
MAC Address Format	M AC address format	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) , eg 00d0f8aabbcc

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



parameter	reference - do not translate	illustrate
802.1x Authentication	802.1x certification	When enabled, the selected interface will enable 8.02.1x authentication .

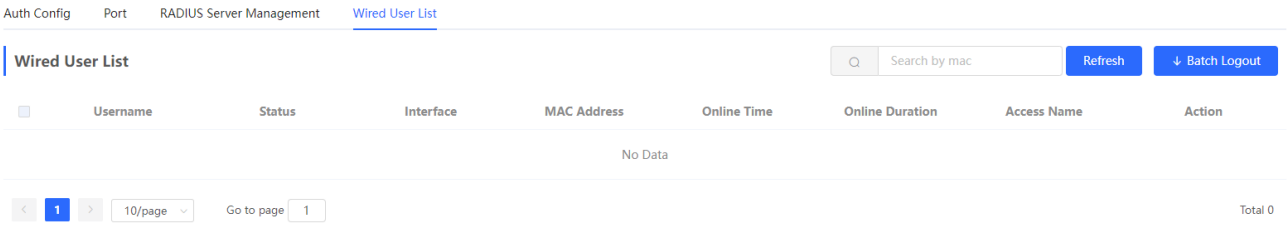
parameter	reference - do not translate	illustrate
Auth Method	authentication method	disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication switch force- auth : Mandatory authentication , the client can directly access the Internet without a password force- unauth : Force no authentication, the client cannot be authenticated, nor can it 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	authentication 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 Internet single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication
Guest Vlan	Guest VLAN	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN Notice 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

parameter	reference - do not translate	illustrate
User Count Limit per Port	Maximum number of users per port	Limit the number of users under the interface Product Difference Description The value range of NBS3100 series switches is 1-256 , and other switches are 1-1000

12.5.3 View the list of wired authentication users

8.02.1x 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.

[Local Management - Page Wizard] Security Management >> 802.1x Authentication to obtain specific user information.



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>.

12.6 Anti-ARP Spoofing

12.6.1 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. 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.

12.6.2 Procedure

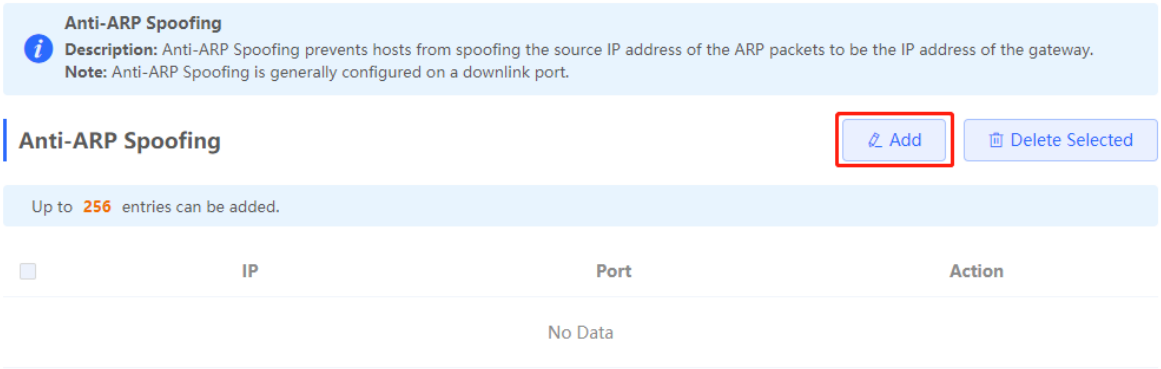
Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN** .

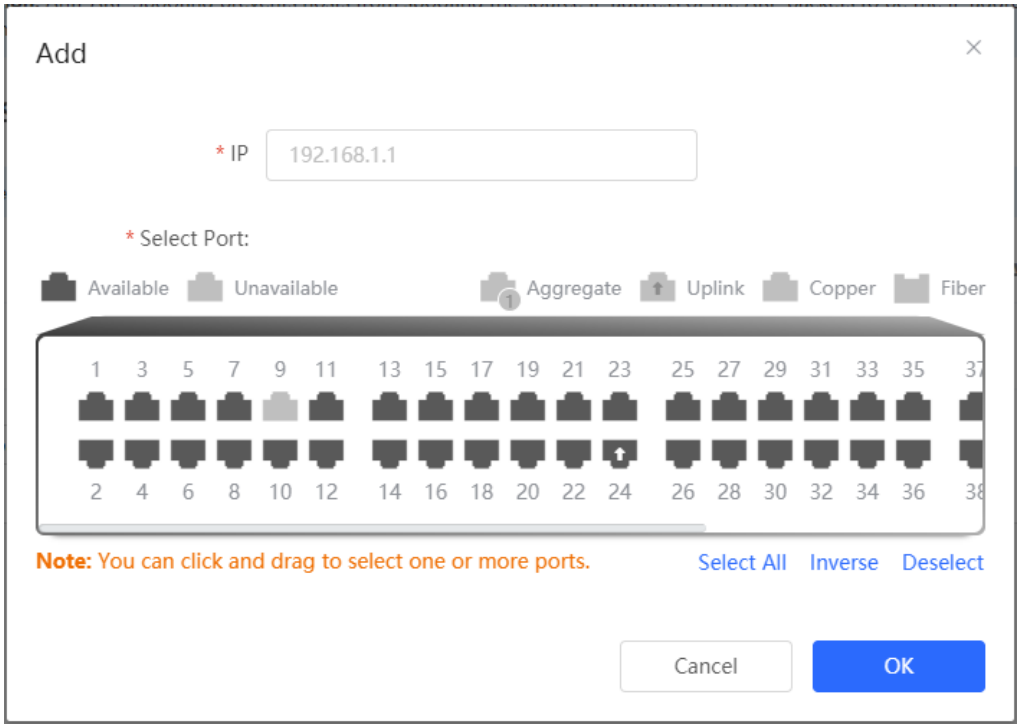
1. Enabling Anti-ARP Spoofing

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.

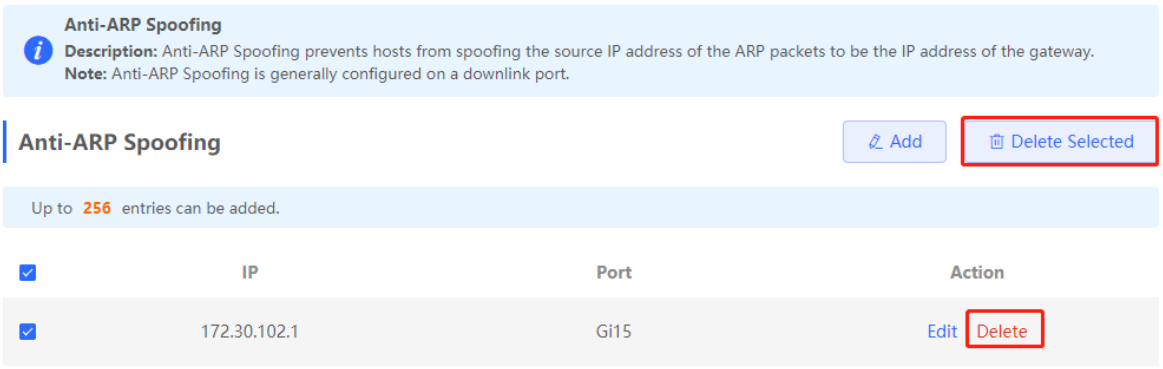




2. Disabling Anti-ARP Spoofing

Batch disable: Select an entry to be deleted in the list and click **Delete Selected** .

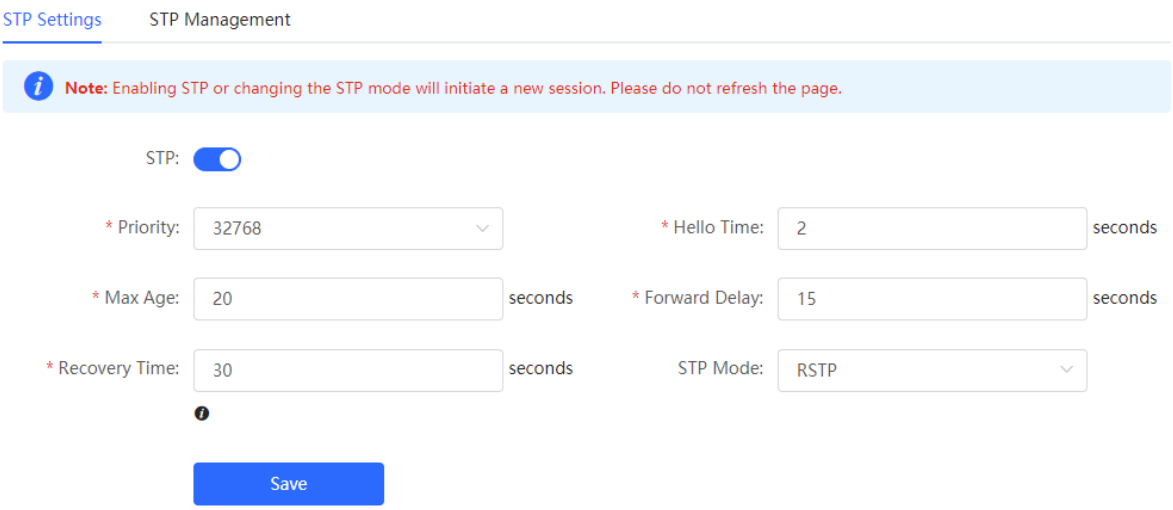
Disable one port: click **Delete** in the last **Action** column of the corresponding entry.



13 Advanced Configuration

13.1 STP

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



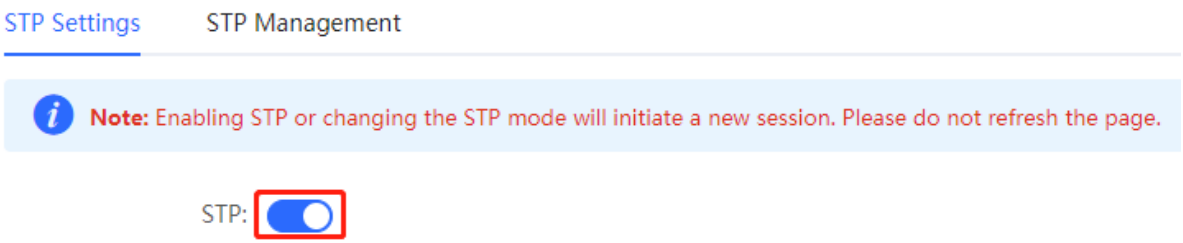
13.1.1 STP Global Settings

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

Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.



(2) Configure the STP global parameters, and click **Save** .

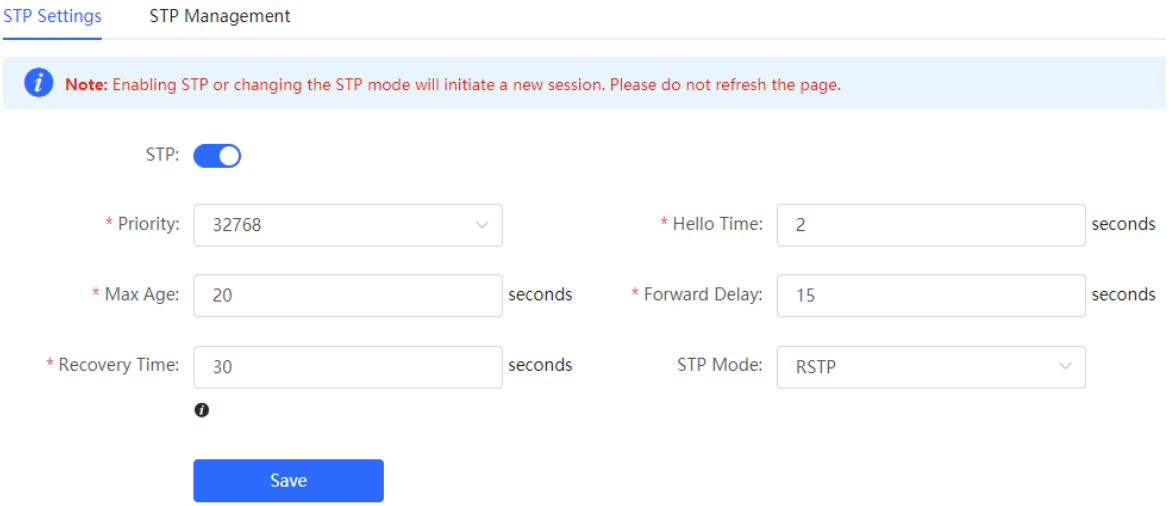


Table 10-7 Description of STP Global Configuration Parameters

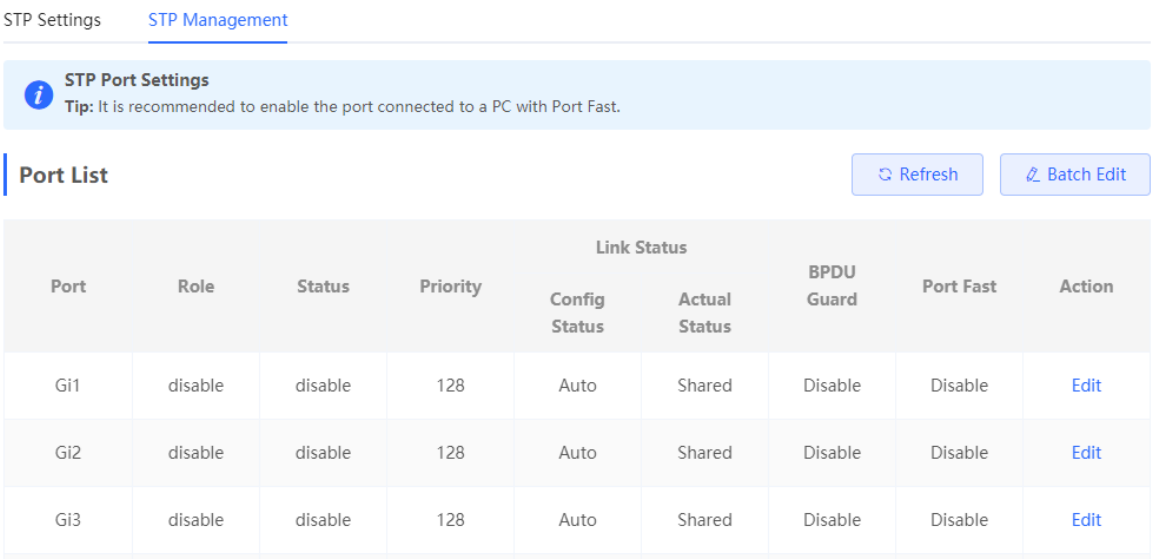
Parameter	Description	Default Value
STP	Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled.	Disable
priority	Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher 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

Parameter	Description	Default Value
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

13.1.2 Applying STP to a Port

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

Configure the STP properties for a port Click **Batch Edit** to select ports and configure STP parameters, or click **Edit** in the **Action** column in **Port List** to configure designated ports.



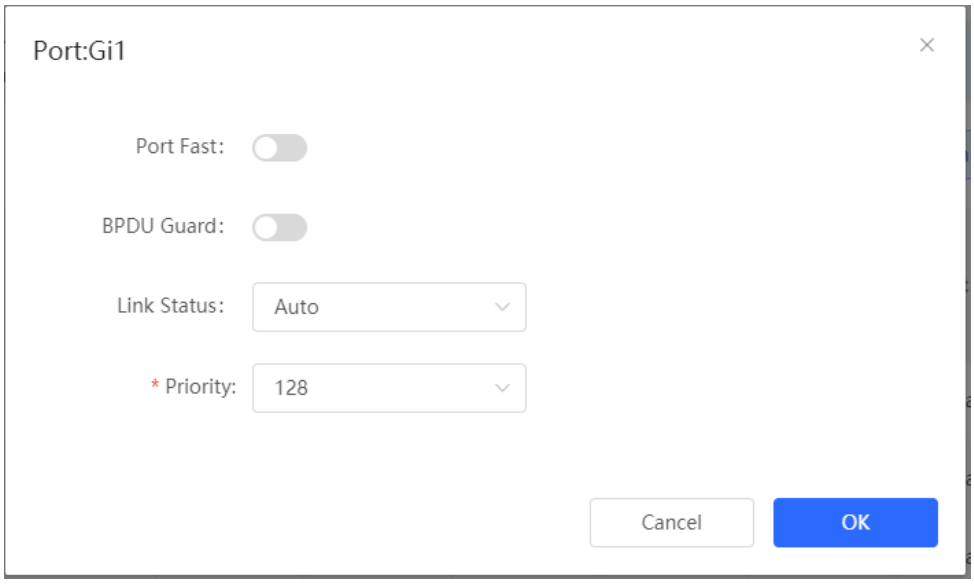


Table 10-8 Description of STP Configuration Parameters of Ports

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.	NA

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.	NA
priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Link Status Config 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	NA
BPDU Guard	Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port connected to an endpoint, but the port receives BPDUs, the port will be disabled and enters the Error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change.	Disable

Parameter	Description	Default Value
Port Fast	Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDU.s. If a port, on which Port Fast is enabled exits the Port Fast state automatically when it receives BPDUs, the BPDU filter feature is automatically disabled. Generally, the port connected to a PC is enabled with Port Fast.	Disable

note

- It is recommended to enable Port Fast on the port connected to a PC.
- A port switches to the forwarding state after STP is enabled more than 30 seconds. Therefore transient disconnection may occur and packets cannot be forwarded.

13.2 LLDP

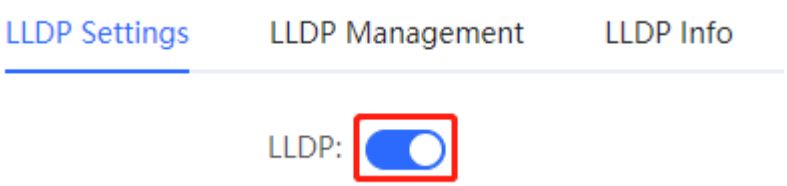
13.2.1 Overview

LLDP (LINK Layer Discovery Protocol) is defined by ieee 802.1ab. LLDP Can Discover Devices and Detect Topology CHANGES. With LLDP, The EWEB Management System M Can Learn The Topology 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.

13.2.2 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.



(2) Configure the global LLDP parameters and click **Save** .

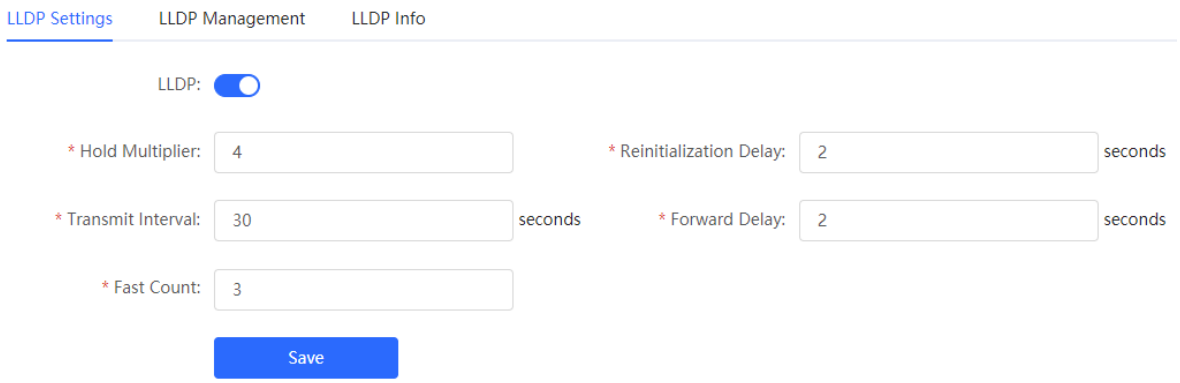


Table 10-9 Description of LLDP Global Configuration Parameters

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

Parameter	Description	Default Value
Forward Delay	Delay for sending LLDP packets, in seconds. When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information. If the delay is set to a very small value, frequent change of the local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed. Set an appropriate delay according to actual conditions.	2 seconds

13.2.3 Applying LLDP to a Port

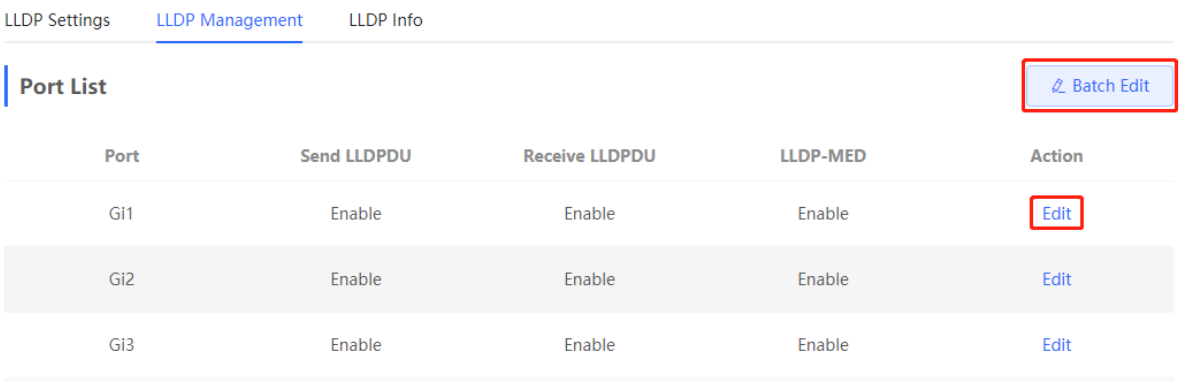
Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Management** .

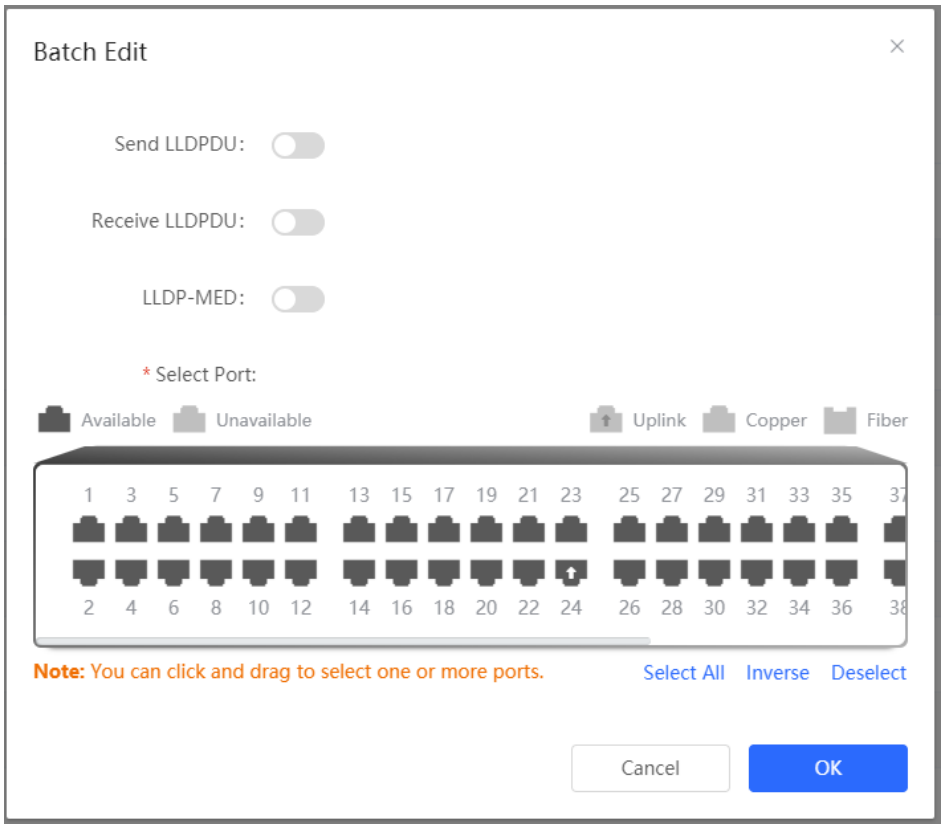
In **Port List** , Click **Edit** in the **Action** column, or click **Batch Edit** , select the desired port, configure the LLDP working mode on the port and whether to enable LLDP-MED, and click **OK** .

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).



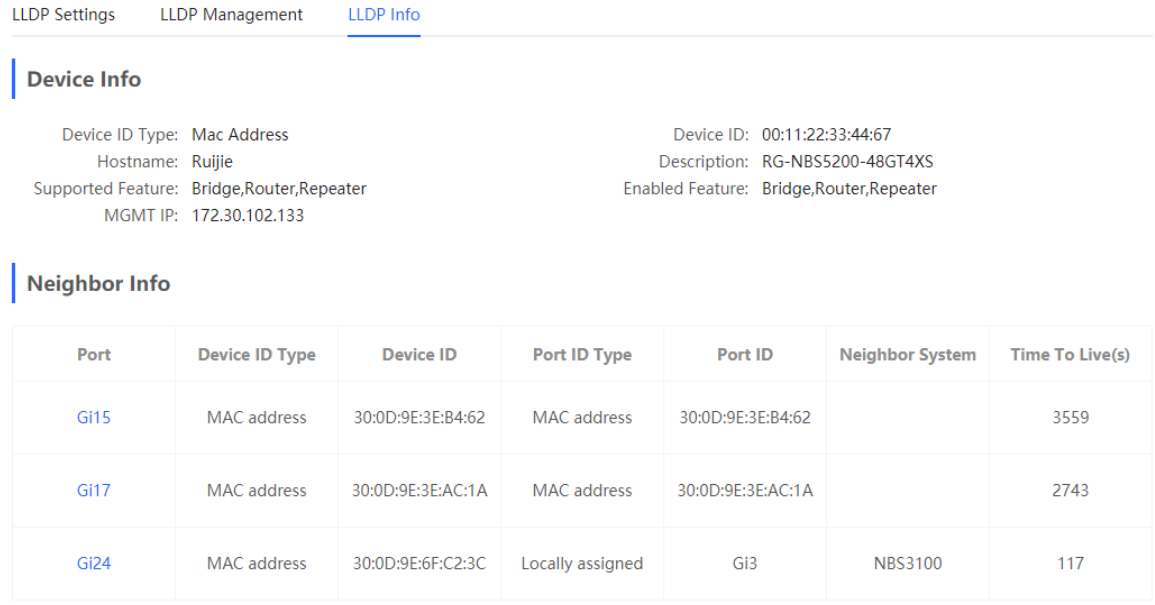


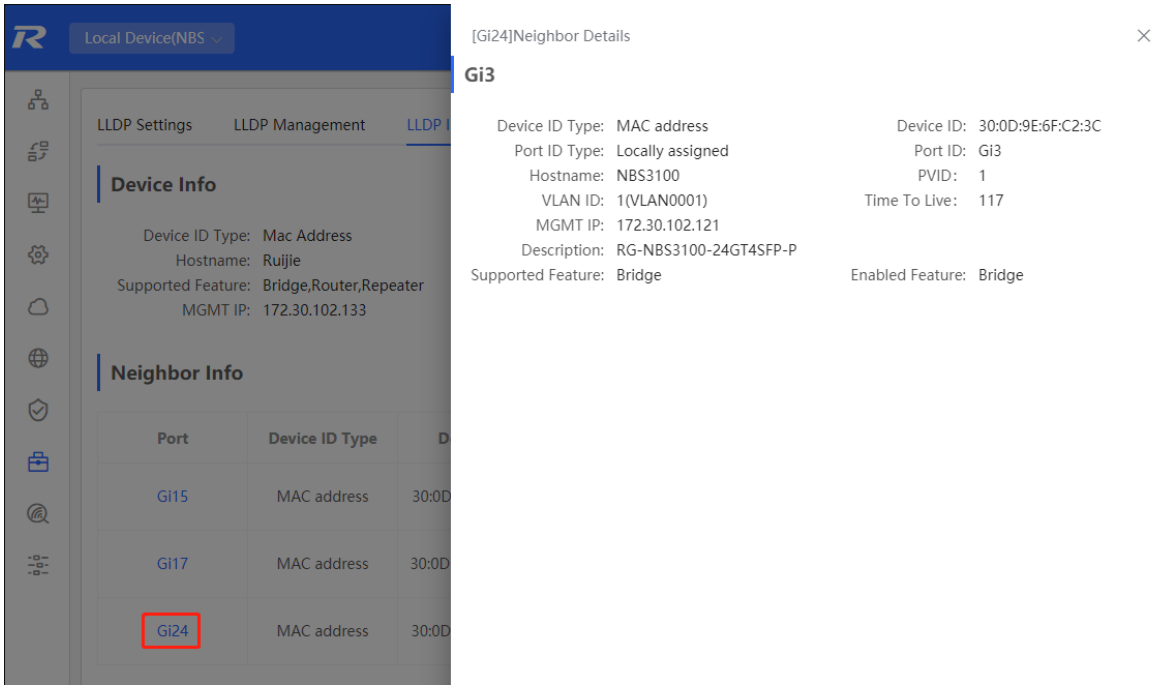
13.2.4 Displaying LLDP information

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 in the network topology. When an administrator configures the VLAN, port rate, duplex mode, an error will be prompted ted If the configurations do not match those on the connected neighbor.





13.3 RLDP

13.3.1 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 ask users to manually

shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet L2 loops.

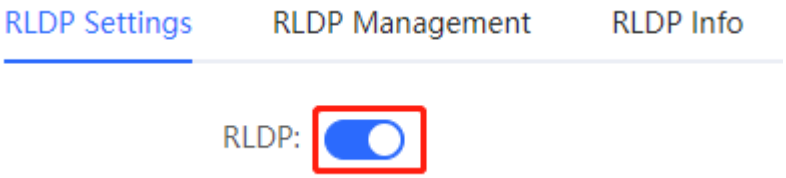
Supports enabling the RLDP function of the access switches in the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and The handling methods after a link fault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

13.3.2 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.



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

Table 10-10 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

Parameter	Description	Default Value
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** .

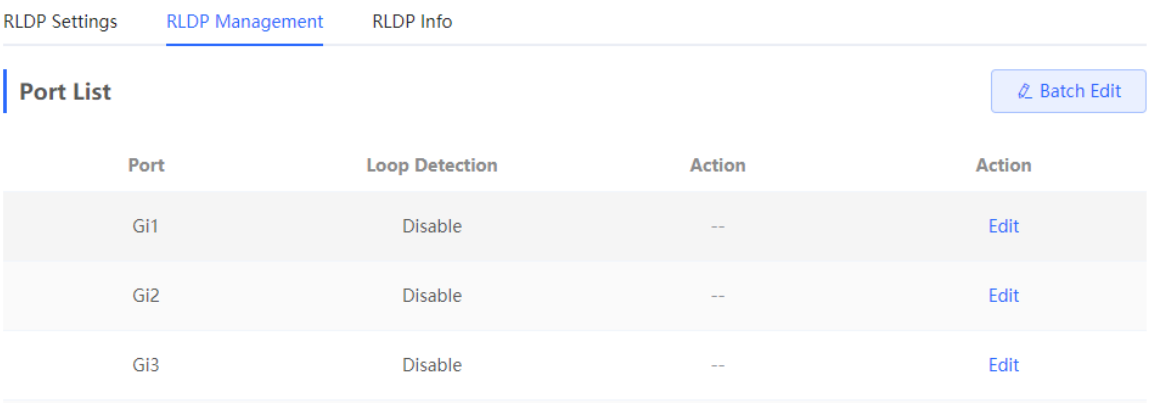
In **Port List,** click **Edit** in the Action column or click **Batch Edit** , select the desired port, configure whether to enable loop detection on the port and the handling method after a fault is detected, and click **OK** .

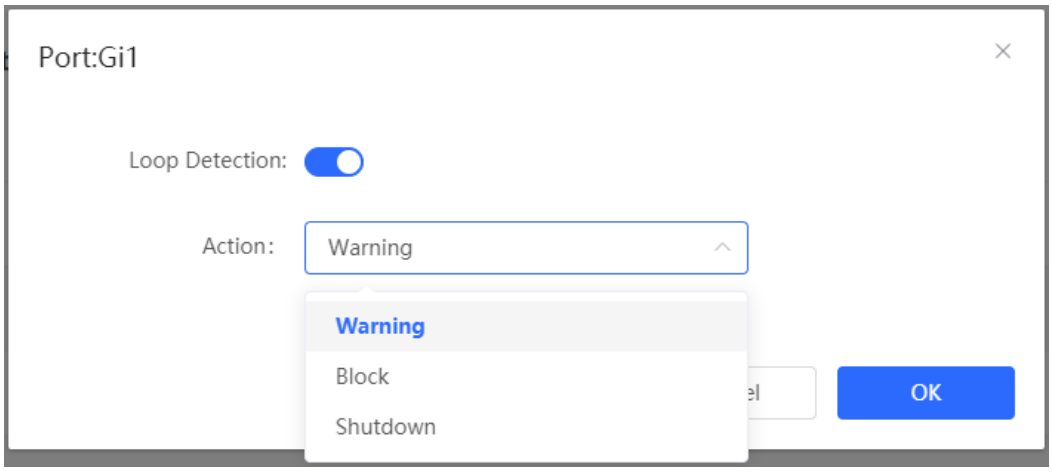
There are three methods to handle port failures:

- 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, shut down 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.

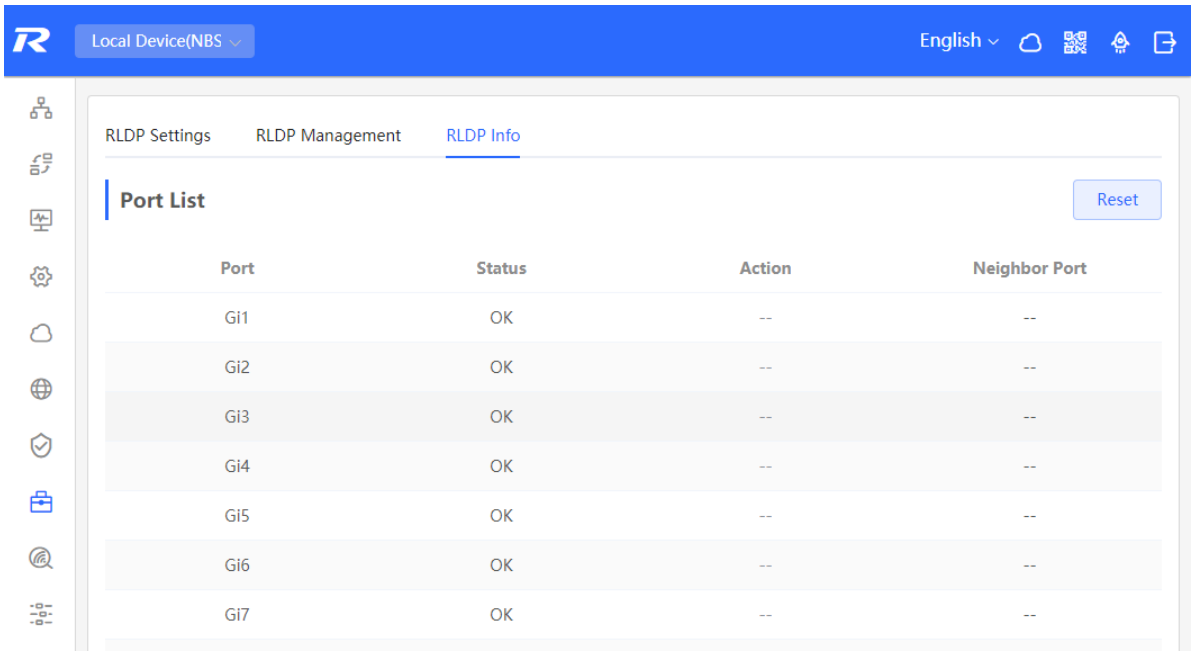




3. Displaying RLDP information

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

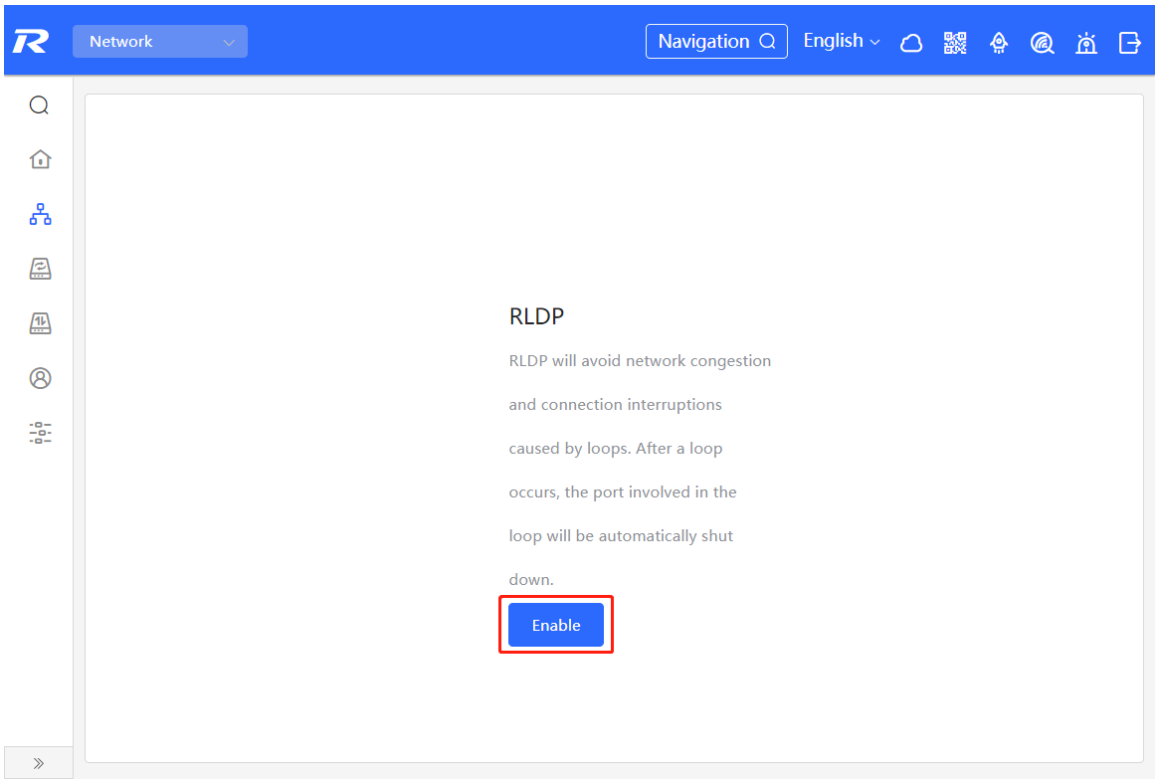
You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDP status triggered by a port to the normal state.



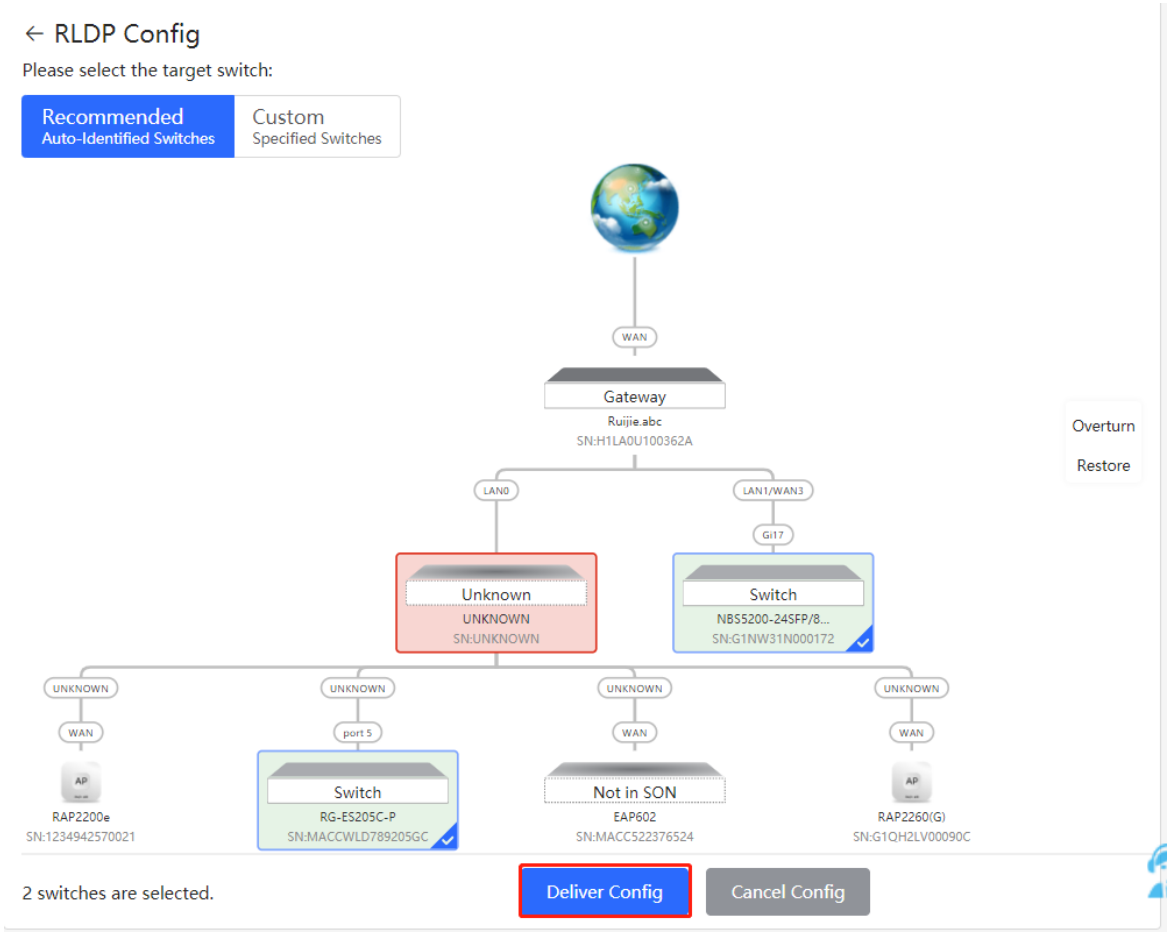
13.3.3 Batch Configuring Network Switches

Choose **Network** > **RLDP** .

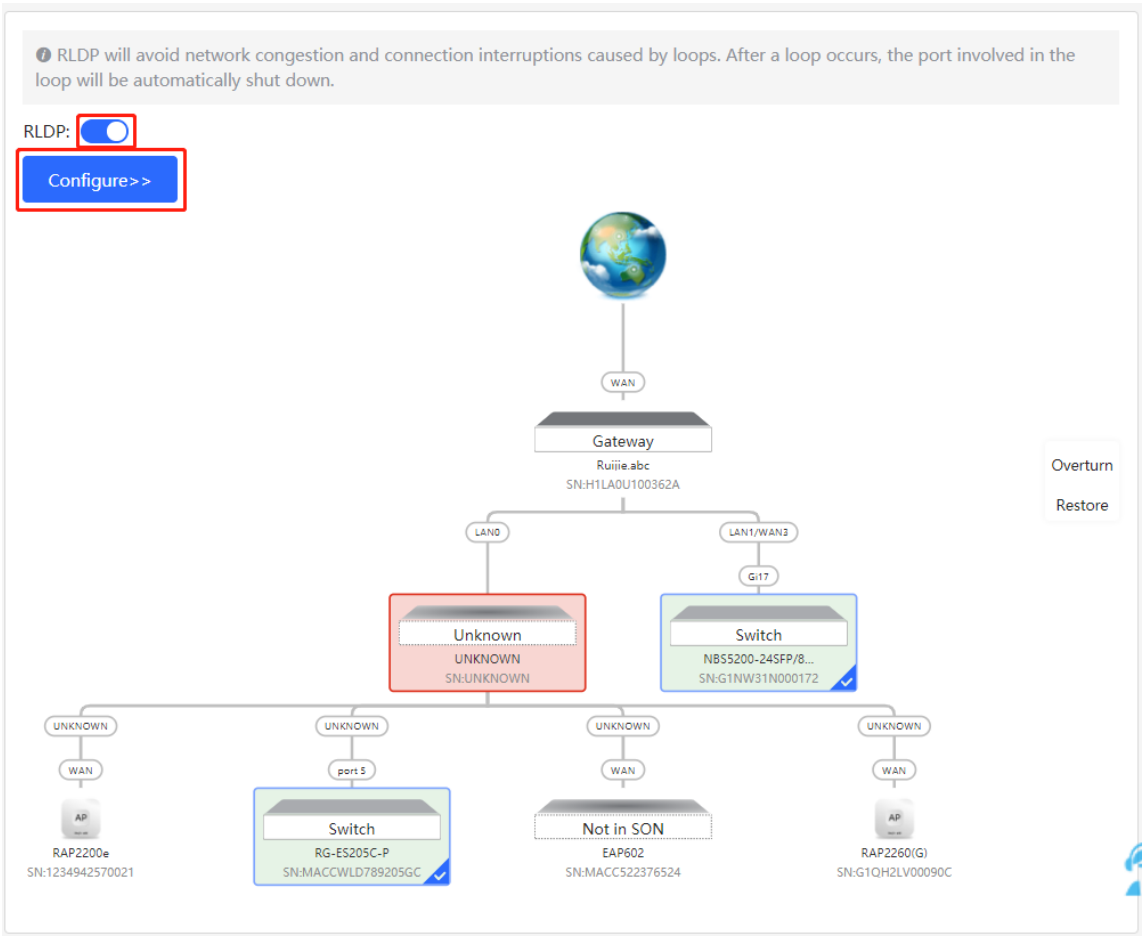
(1) Click **Enable** to access the **RLDP Config** page.



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



(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.

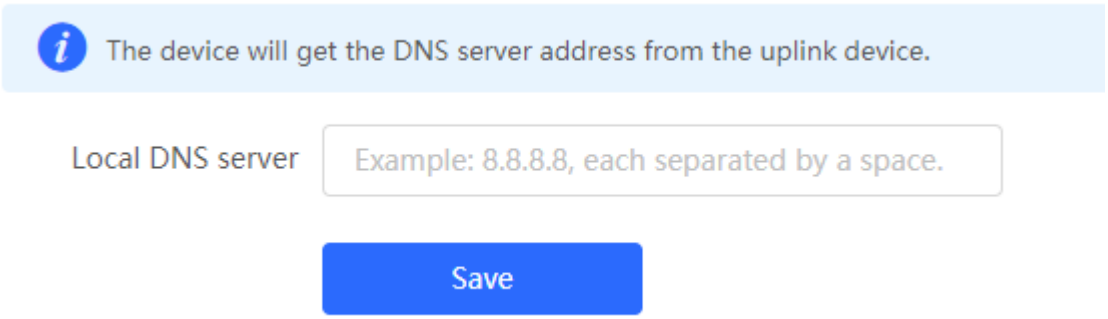


13.4 Configuring the Local DNS

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 resolving domain names. If the device fail To parse domain names, then use this DNS address instead.



13.5 Voice VLAN

Caution

The Voice VLAN function is supported by RG-NBS3100 Series, RG-NBS3200 Series, RG-NBS5100 Series and RG-NBS5200 Series Switches.

13.5.1 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.

13.5.2 Voice VLAN Global Configuration

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

Turn on the voice VLAN function, configure global parameters, and click **Save** .

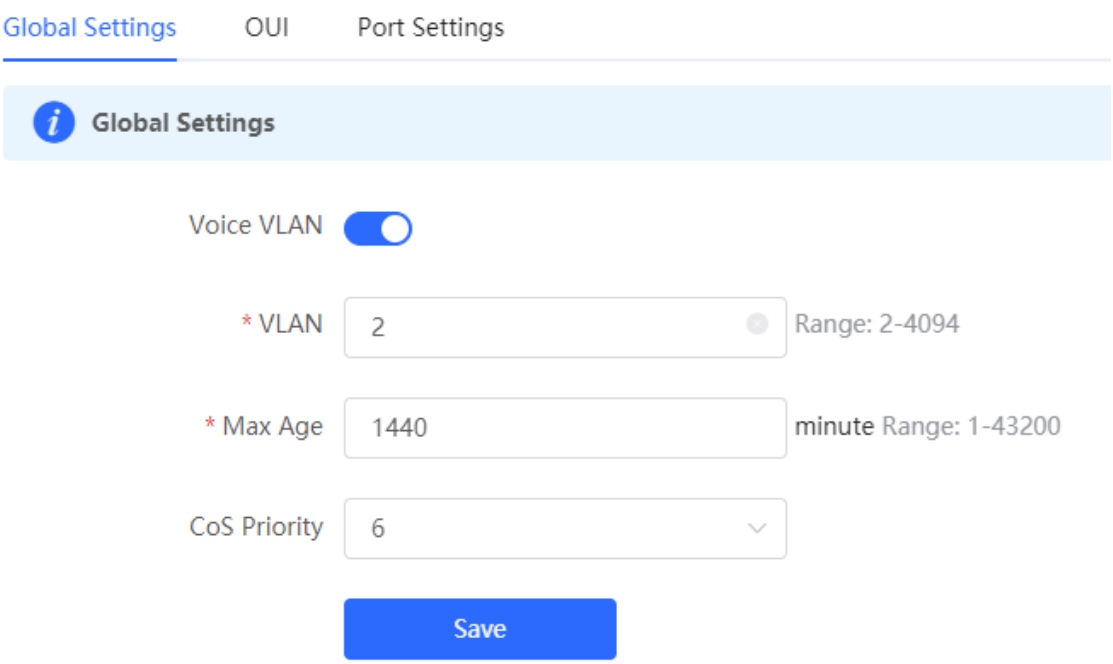


Table 10-11 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable
VLAN	VLAN ID as Voice VLAN	NA
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

13.5.3 Configuring a Voice VLAN OUI

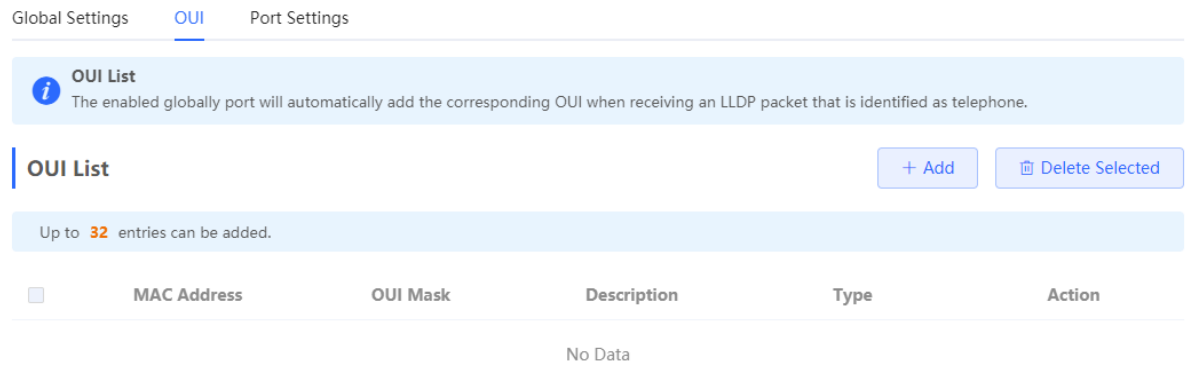
Choose **Local Device** > **Advanced** > **Voice VLAN** > **OUI** .

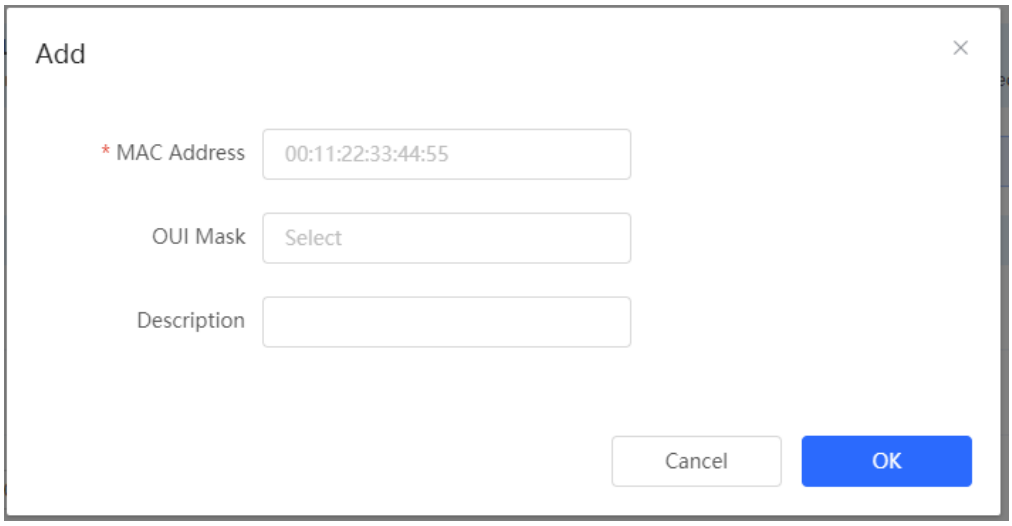
The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and send them 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** .





13.5.4 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** .

Global Settings OUI Port Settings

Port List

The port can be set to the automatic mode only when the port VLAN is in the trunk or hybrid mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.
To ensure the normal operation of voice VLAN on port, please do not switch the port mode (hybrid/trunk/access mode). To switch the mode, please disable the voice VLAN first.
Voice VLAN does not support layer 3 ports and aggregation ports.

Port List Batch Edit

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Disabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit

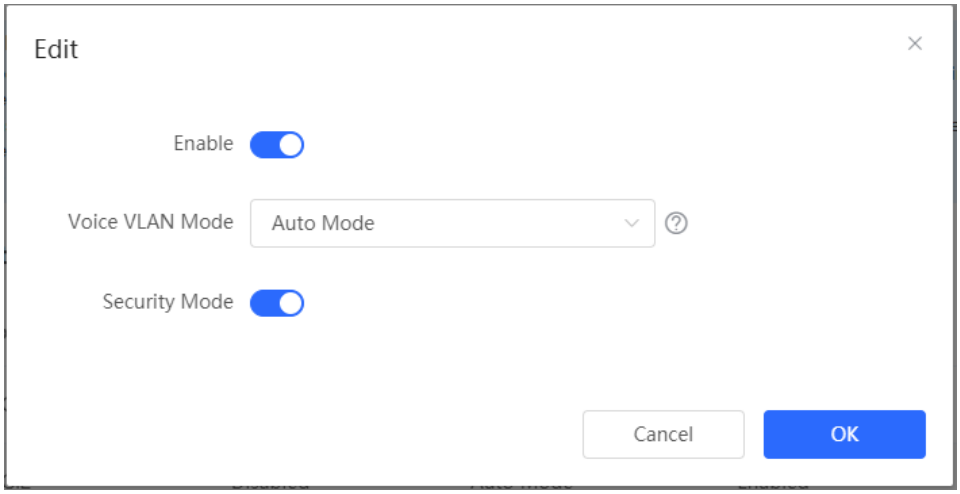


Table 10-12 Description of the Voice VLAN Configuration Parameters on a Port

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.

13.6 Configuring Smart Hot Standby (VCS)

Smart hot standby enables multiple switches to act as a hot standby device for each other, ensuring uninterrupted data forwarding in the event of a single point failure.

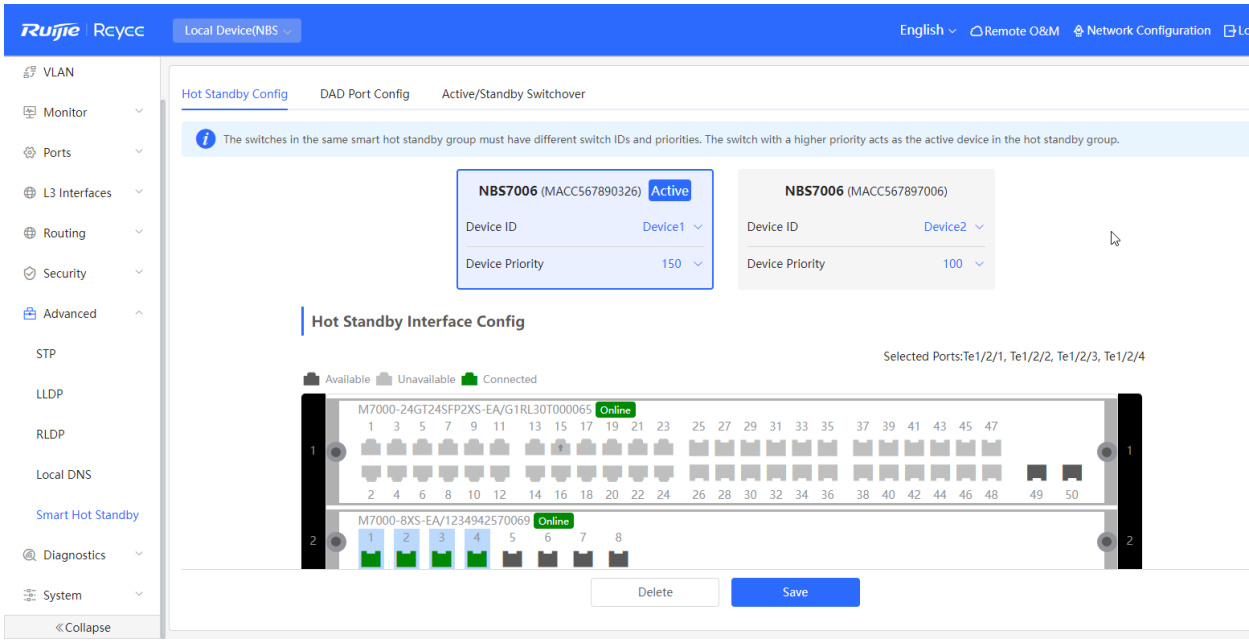
13.6.1 Configuring Hot Standby

View or modify selected hot standby interfaces, device IDs and priorities. The switch with a higher priority is selected as the active switch in a hot standby group.

Caution

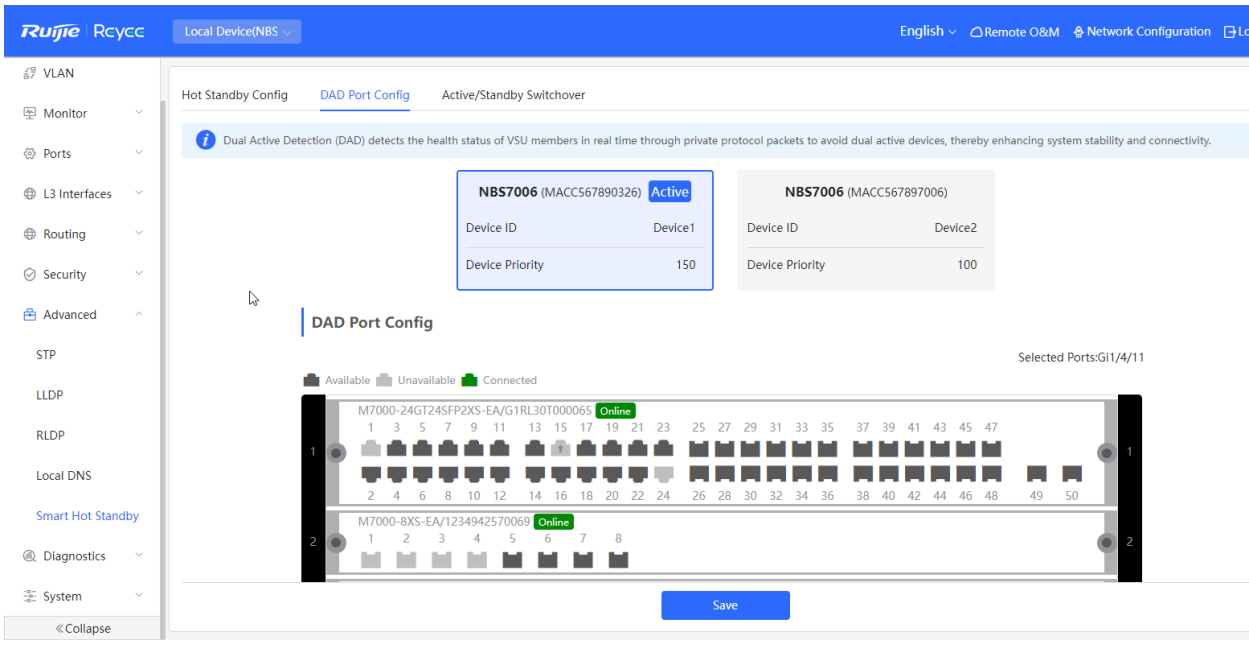
The devices in a hot standby group must have unique device IDs and priorities configured .

Choose **Local Device** > **Advanced** > **Smart Hot Standby** .



13.6.2 Configuring DAD Interfaces

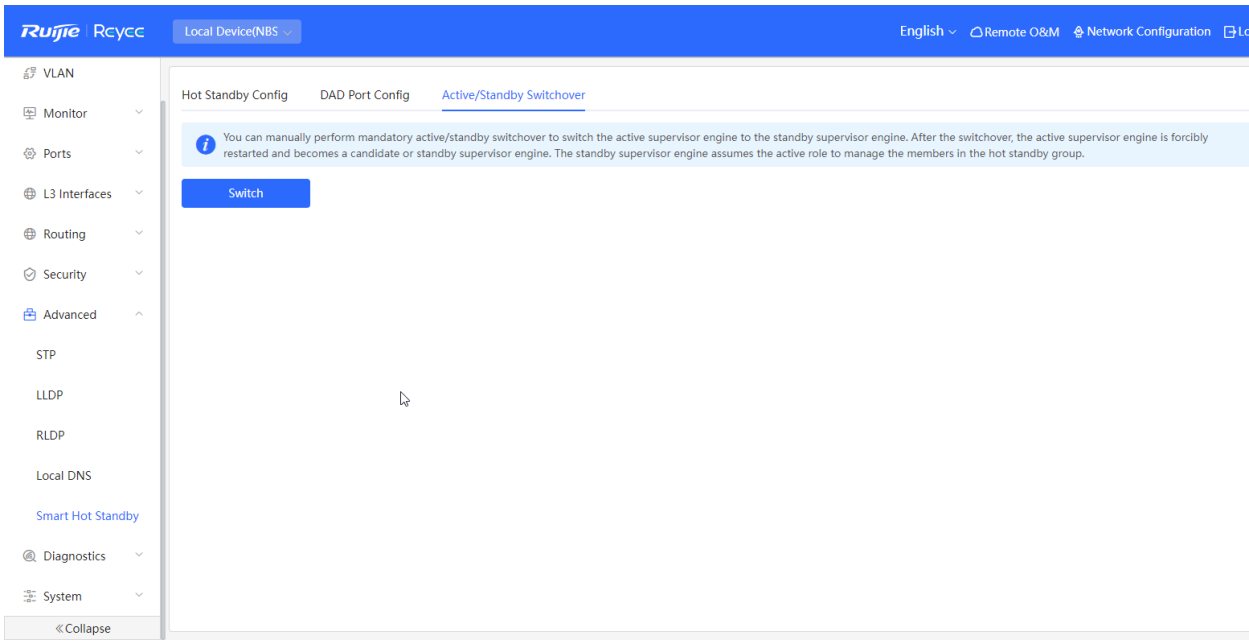
After selecting the DAD interfaces of both the active and standby switches, connect these DAD interfaces with a network cable to prevent network failures caused by dual active devices.



13.6.3 Active/Standby Switchover

Active/Standby Switchover allow manual switching between the active and standby supervisor engines.

Clicking the **Switch** button will restart the supervisor engine. Please exercise caution.

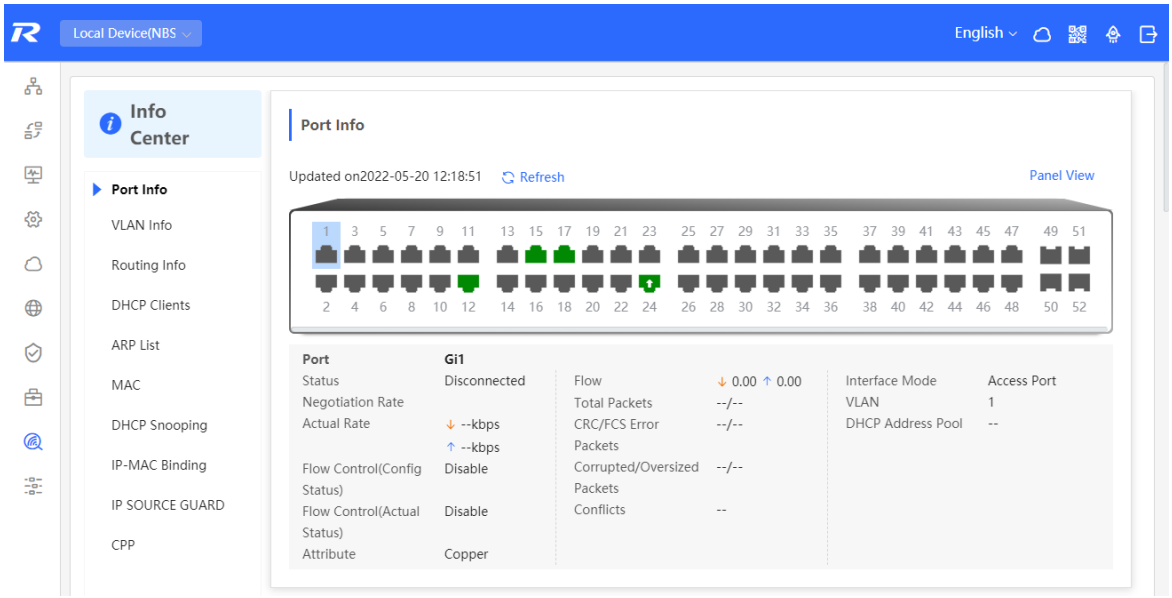


14 Diagnostics

14.1 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.



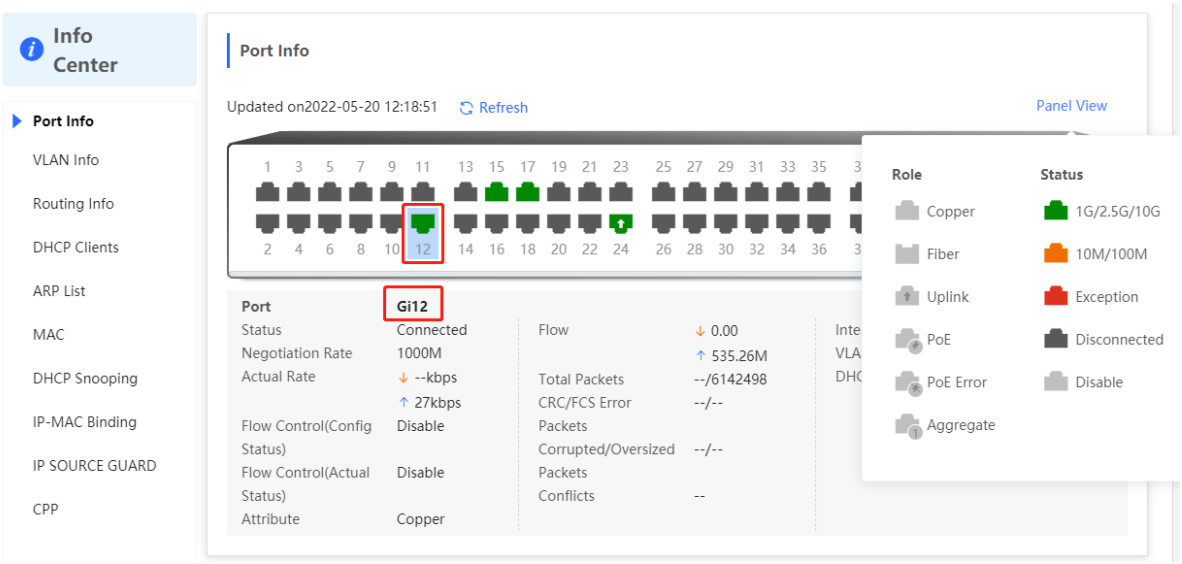
14.1.1 Port Info

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

Port Info displays the status and configuration information of the port. Click the port icon to view the detailed information of the port.

note

- To configure the flow control of the port or the optical/electrical attribute of a combo port, see 4.2 .
- To configure the L2 mode of the port and the VLAN to which it belongs, see 3.5.3 .



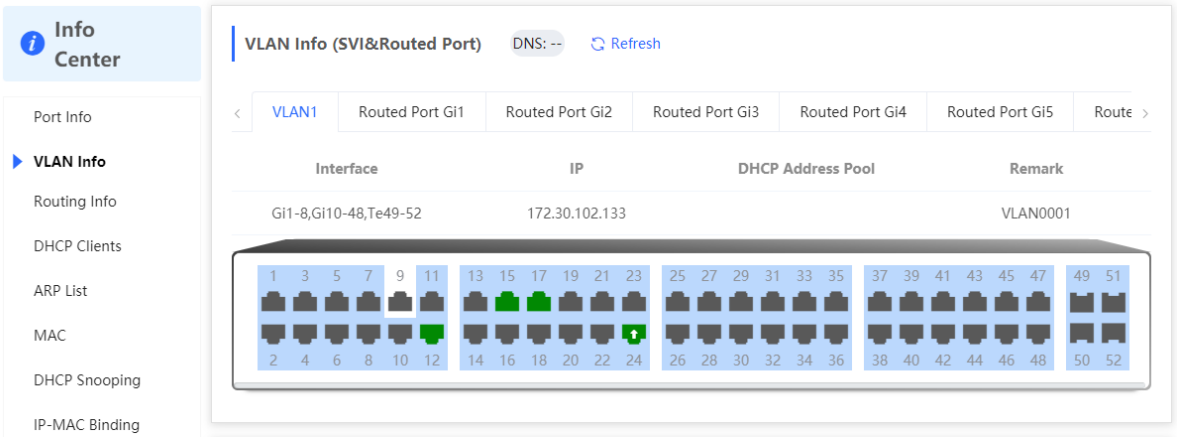
14.1.2 VLAN Info

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 3.5 .
- To configure SVI ports and routed ports, see 6.1 .



14.1.3 Routing Info

Caution

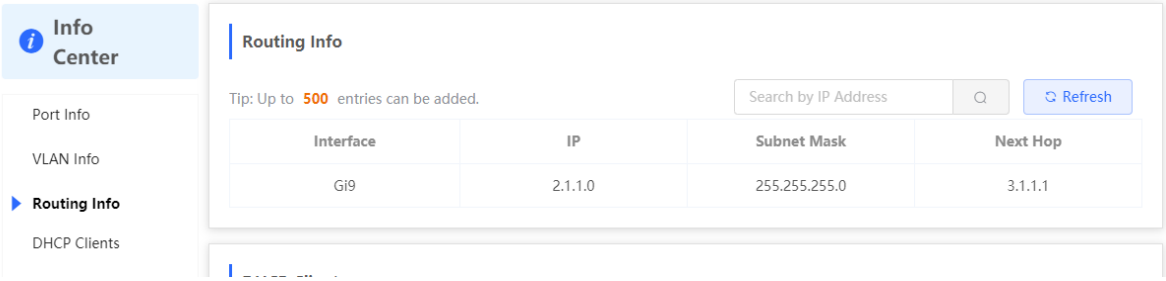
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

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

Displays the routing information on the device. The search box in the upper-right corner supports finding route entries based on IP addresses.

note

To set up static routes, see 6.3 .



14.1.4 DHCP Clients

Caution

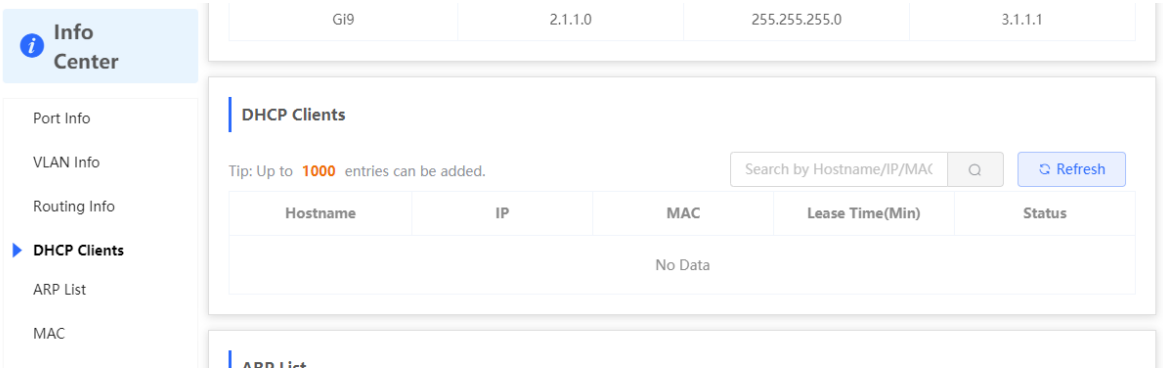
If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), this type of information is not displayed.

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Clients** .

Displays the IP address information assigned to endpoints by the device as a DHCP server.

note

To configure DHCP server related functions, see 6.2 .



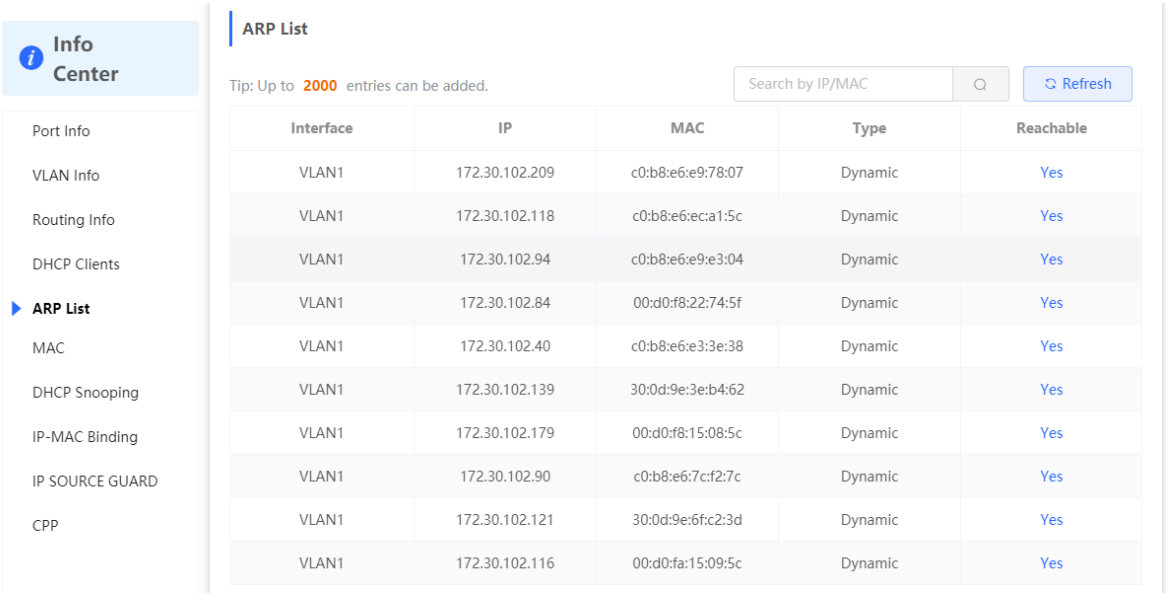
14.1.5 ARP List

Choose **Local Device** > **Diagnostics** > **Info Center** > **ARP List** .

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

note

To bind dynamic ARP or manually configure static ARP, see 6.4 .



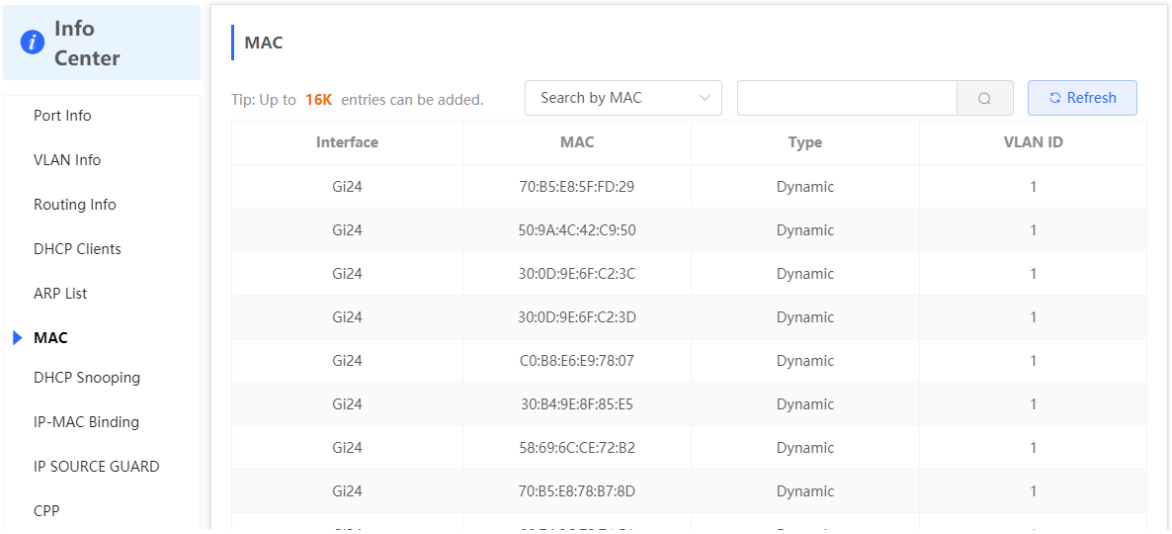
14.1.6 MAC Address

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

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

note

To configure and manage the MAC address, see 3.3 .



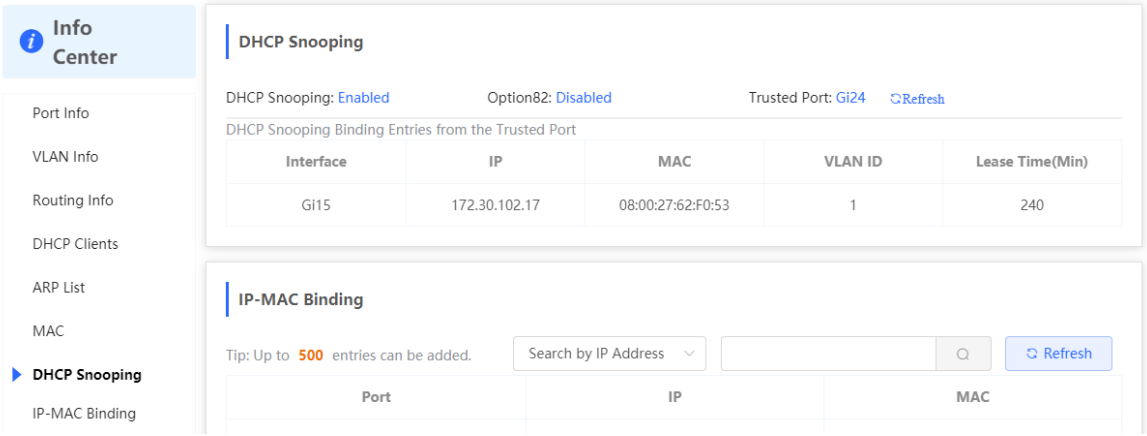
14.1.7 DHCP Snooping

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Snooping** .

Displays the current configuration of the DHCP snooping function and the user information dynamically learned by the trust port.

note

To modify DHCP Snooping related configuration, see 7.1 .



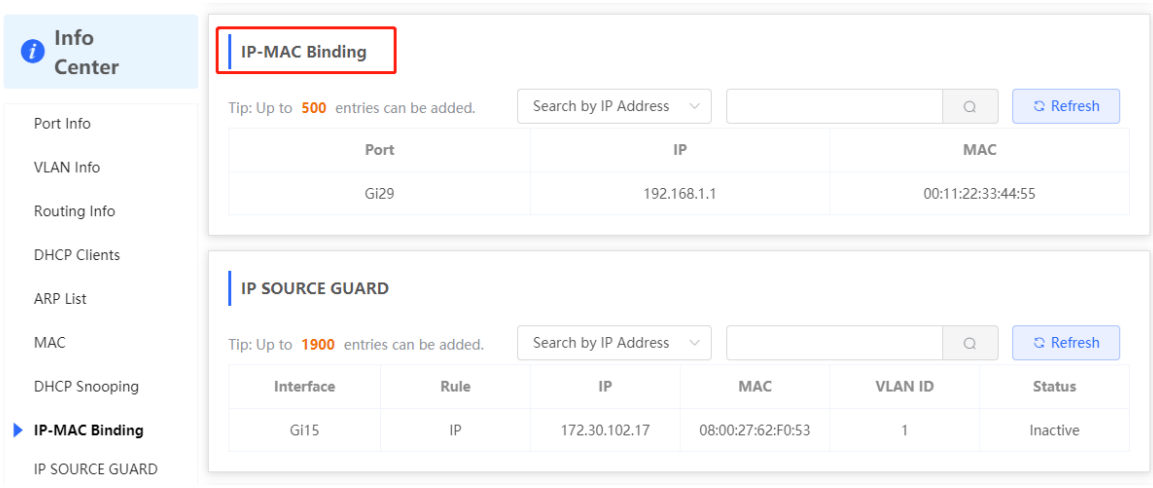
14.1.8 IP-MAC Binding

Choose **Local Device** > **Diagnostics** > **Info Center** > **IP-MAC Binding** .

Displays the configured IP-MAC binding entries. The device checks whether the source IP addresses and source MAC addresses of IP packets match those configured for the device and filters out IP packets not matching the binding.

note

To add or modify the IP-MAC binding, see 7.5 .



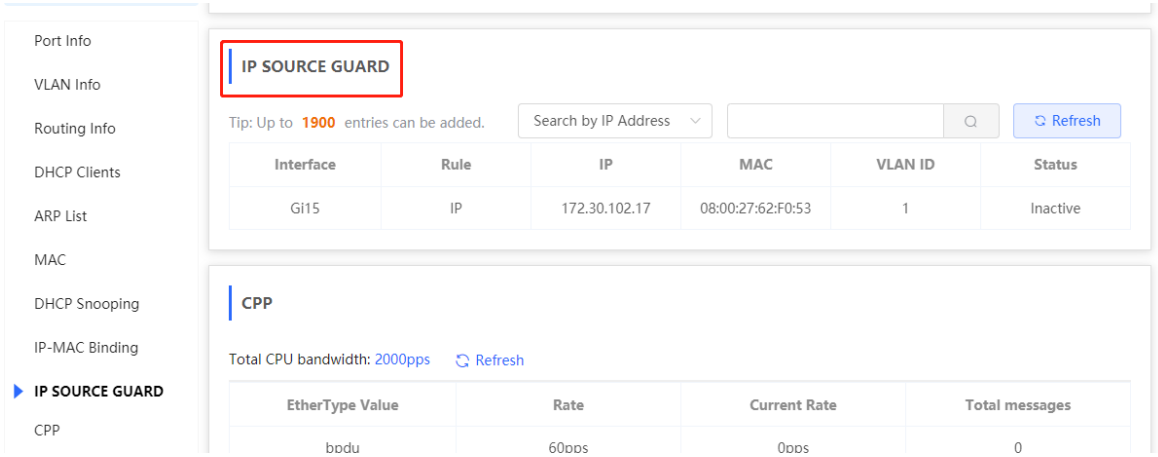
14.1.9 IP Source Guard

Choose **Local Device** > **Diagnostics** > **Info Center** > **Source Guard** .

Displays the binding list of the IP Source Guard function. The IP Source Guard function will check the IP packets from non-DHCP trusted ports according to the list, and filter out the IP packets that are not in the binding list.

note

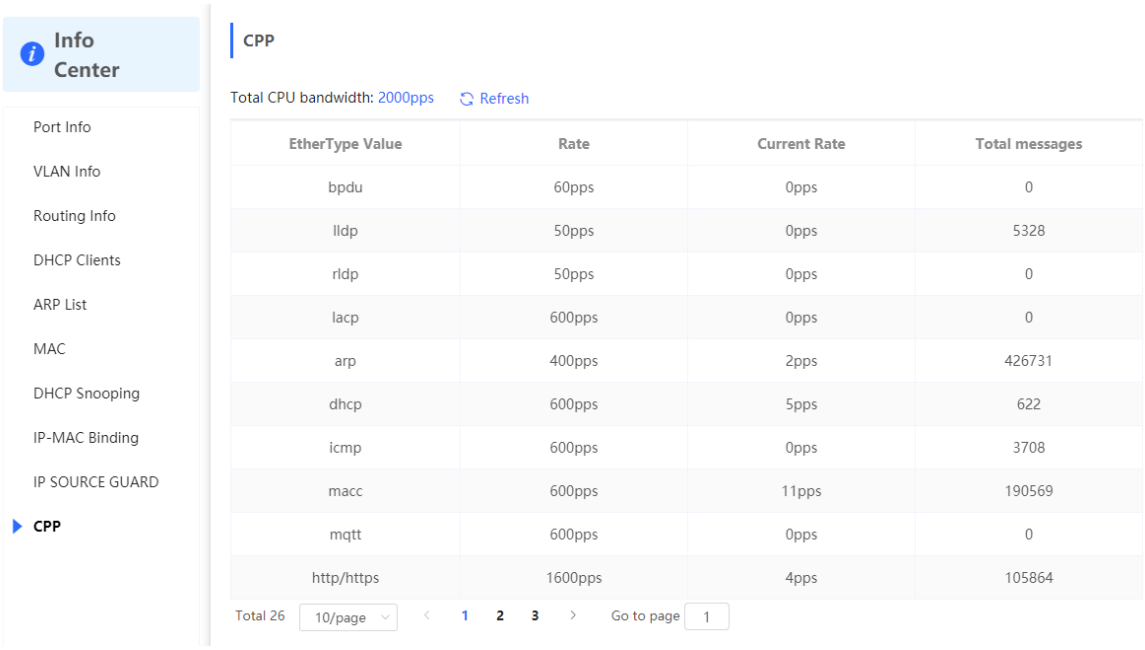
To configure IP Source Guard function, see 7.6 .



14.1.10 CPP Info

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

Displays the current total CPU bandwidth and statistics of various packet types, including the bandwidth, current rate, and total number of packets.



14.2 Network Tools

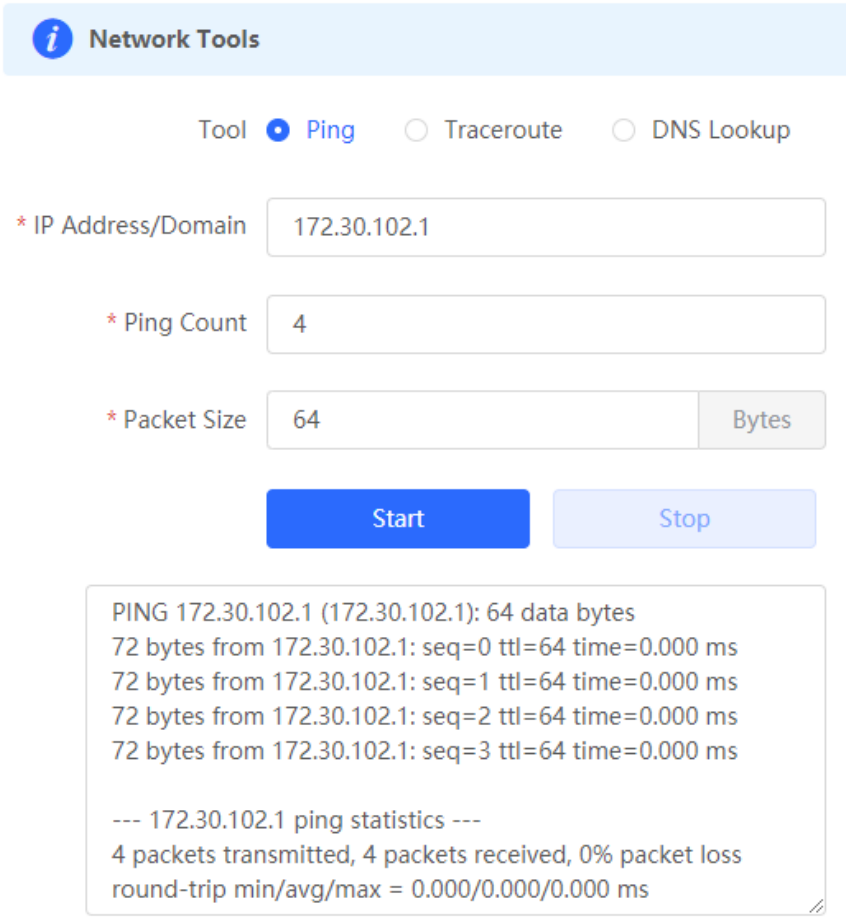
The **Network Tools** page provides three tools to detect the network status: **Ping** , **Traceroute** , and **DNS Lookup** .

14.2.1 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.

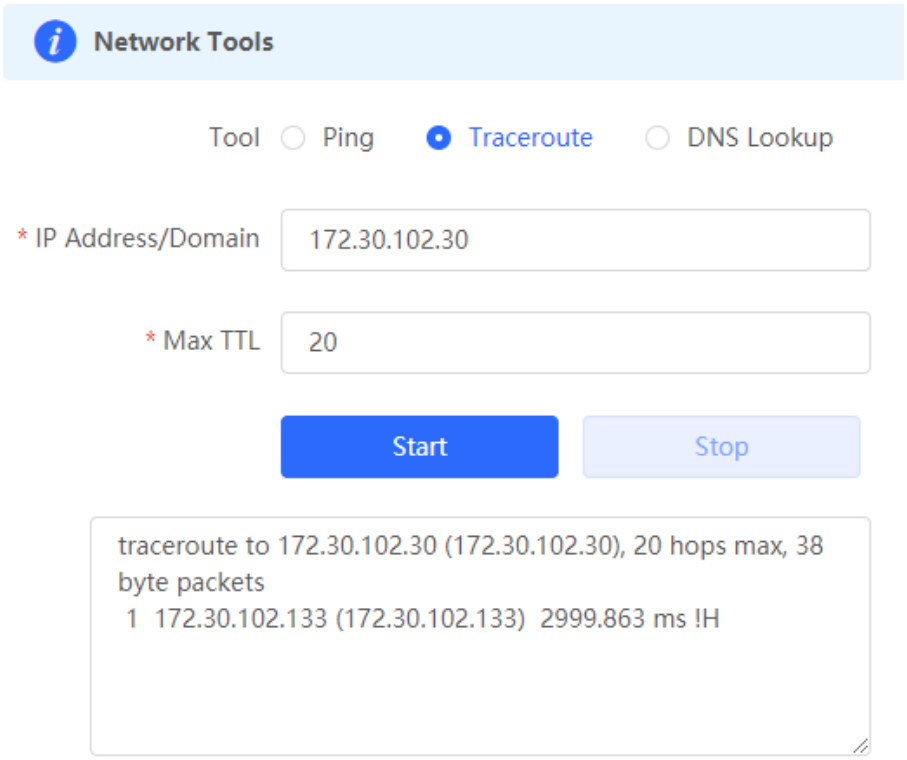


14.2.2 Traceroute

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** .

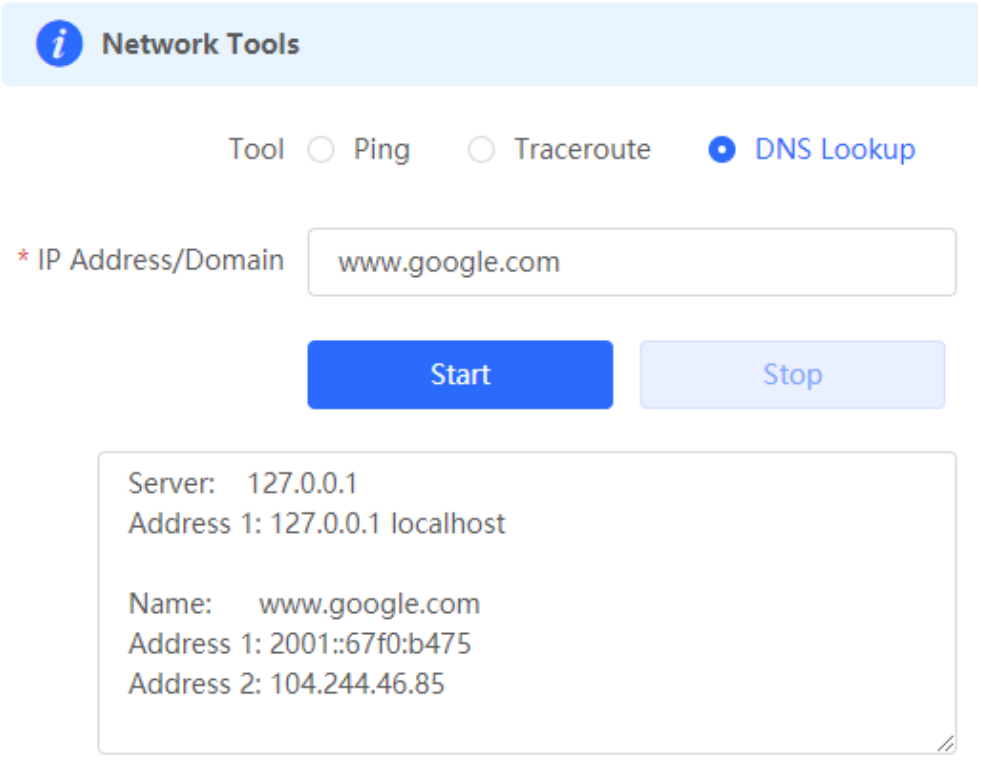


14.2.3 DNS Lookup

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.

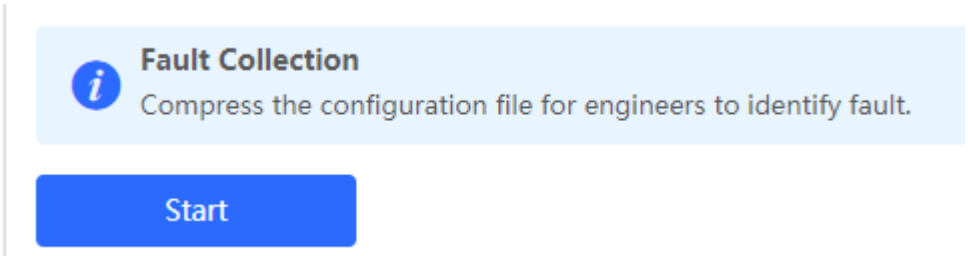
Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and click **Start** .



14.3 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.

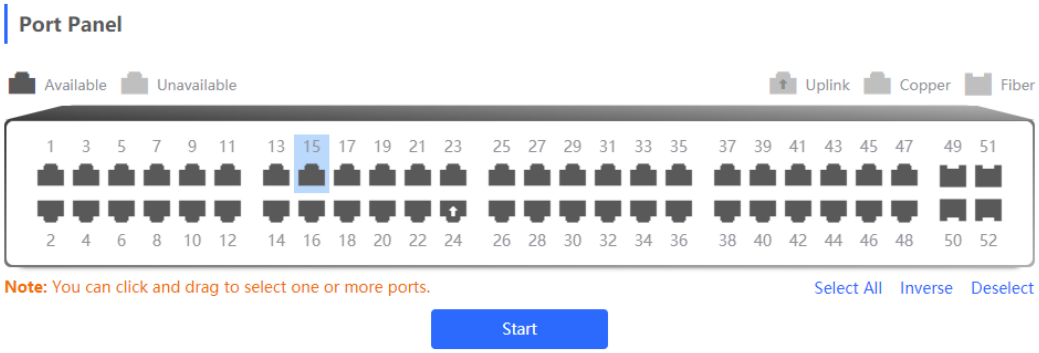


14.4 Cable Diagnostics

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.



Result

Port	Cable Length (cm)	Result
Gi15	700	OK

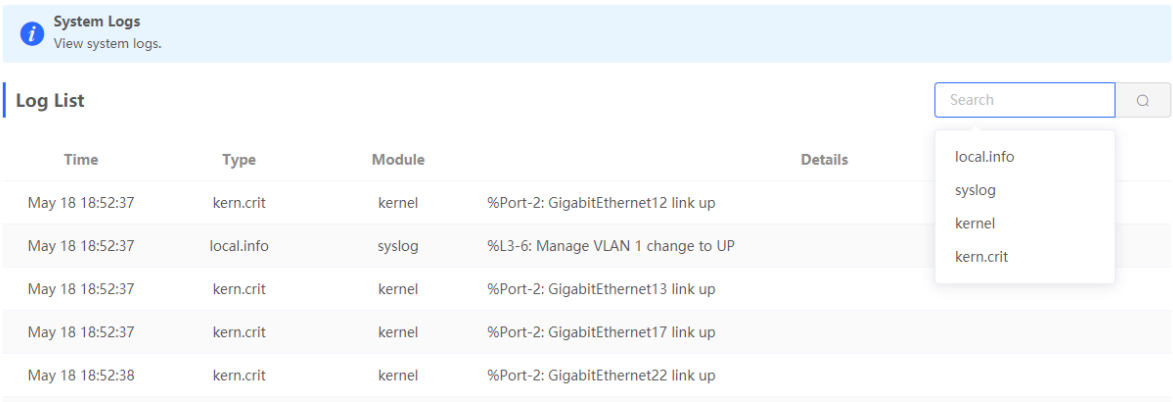
Caution

- The SPF port does not support the function.
- If a detected port contains an uplink port, the network may be intermittently disconnected. Exercise caution when performing this operation.

14.5 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.



14.6 Alerts

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

note

Choose **Network** > **Alerts** to view the alert information of other devices in the network.

Displays possible problems on the network environment to facilitate fault prevention and troubleshooting. You can view the alert occurrence time, port, alert impact, and handling suggestions, and rectify device faults according to handling suggestions.

All types of alerts are concerned by default. You can click **Unfollow** to unfollow this type of alert. The system will no longer display this type of alert. To enable the notification function of a type of alert again, follow the alert type on the **Removed Alert** page.

Caution

After unfollowing an alert, the system will not issue an alert prompt for this type of fault, and users cannot find and deal with the fault in time. Exercise caution when performing this operation.

Table 11-2 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series, RG-NBS3200 Series Switches do not support this type of alert.

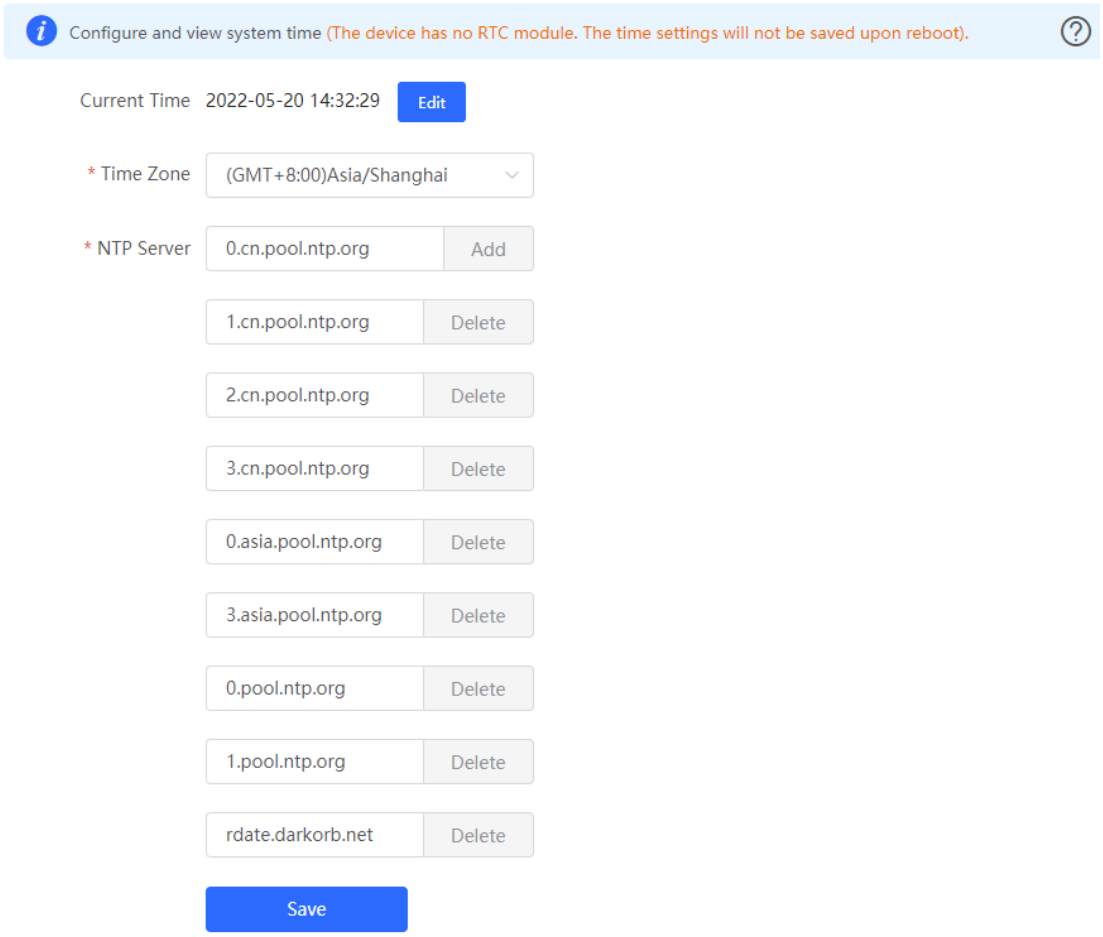
Alert Type	Description	Support Description
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	NA
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	NA
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of the product.	NA
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	NA
The PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and the new connected PD cannot be powered properly.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	NA

15 System Configuration

15.1 Setting the System Time

Choose **System** > **System Time** .

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click Edit to manually set the time. In addition, the device supports **Network** Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.



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

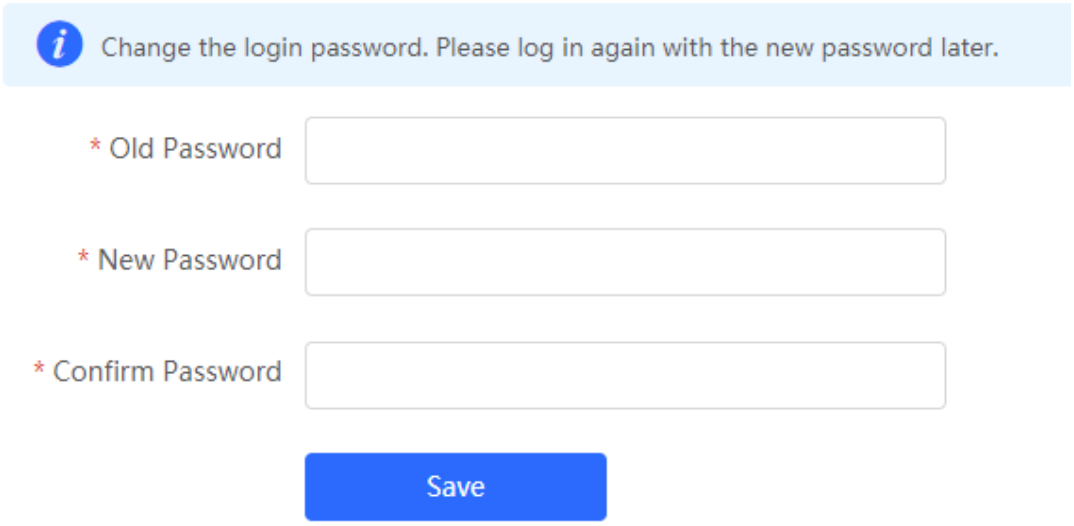
15.2 Setting the Web Login Password

Choose **System** > **Login** > **Login Password** .

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.



15.3 Setting the Session Timeout Duration

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

If you do not log out after login, the Eweb management system allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the

Eweb management system automatically refreshes the page and you need to relog in before continuing your operations. You can change the session timeout duration.

15.4 Configuring SNMP

15.4.1 Overview

SNMP (Simple Network Management Protocol) is a protocol used for managing network devices. It is based on the client/server model and can remotely monitor and control network devices.

SNMP consists of a management station and agents, with the management station communicating with agents through the SNMP protocol to obtain information such as device status, configuration information, performance data, etc., while also being able to configure and manage devices.

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

15.4.2 Global Configuration

1. Overview

The purpose of global configuration is to enable SNMP services and implement basic configurations such as SNMP protocol version (v1/v2c/v3), local port settings, device location settings, contact information settings.

SNMPv1: v1 is the earliest version of SNMP with poor security that only supports simple community string authentication. The v1 version has some defects such as plaintext transmission of community strings which makes it vulnerable to attacks; therefore it is not re recommended for use in modern networks .

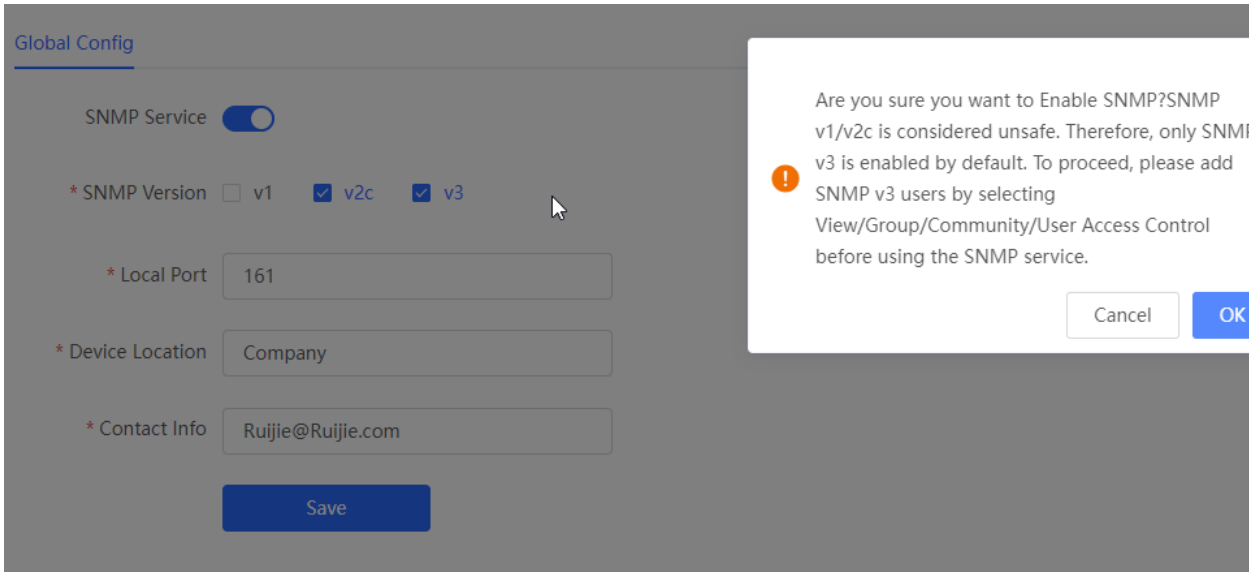
SNMPv2c: v2c is an improved version over v1 that supports richer functionality and more complex data types while enhancing security measures compared to its predecessor. The v2c version provides better security features than v1 along with greater flexibility ity allowing users to configure according to their specific needs.

SNMPv3: This latest version of the SNMP protocol includes additional security mechanisms like message authentication encryption compared to its predecessors - V1 & V2C - resulting in significant improvements in terms of access control & overall safety measures im plemented by this standard.

2. Configuration Steps:

[Network-wide Management-Page Wizard] System >> SNMP>>Global Config

(1) Enable SNMP services.



When first opened, the system prompts to enable SNMPv3 by default. Click < OK >.

(1) Set global configuration parameters for SNMP service.

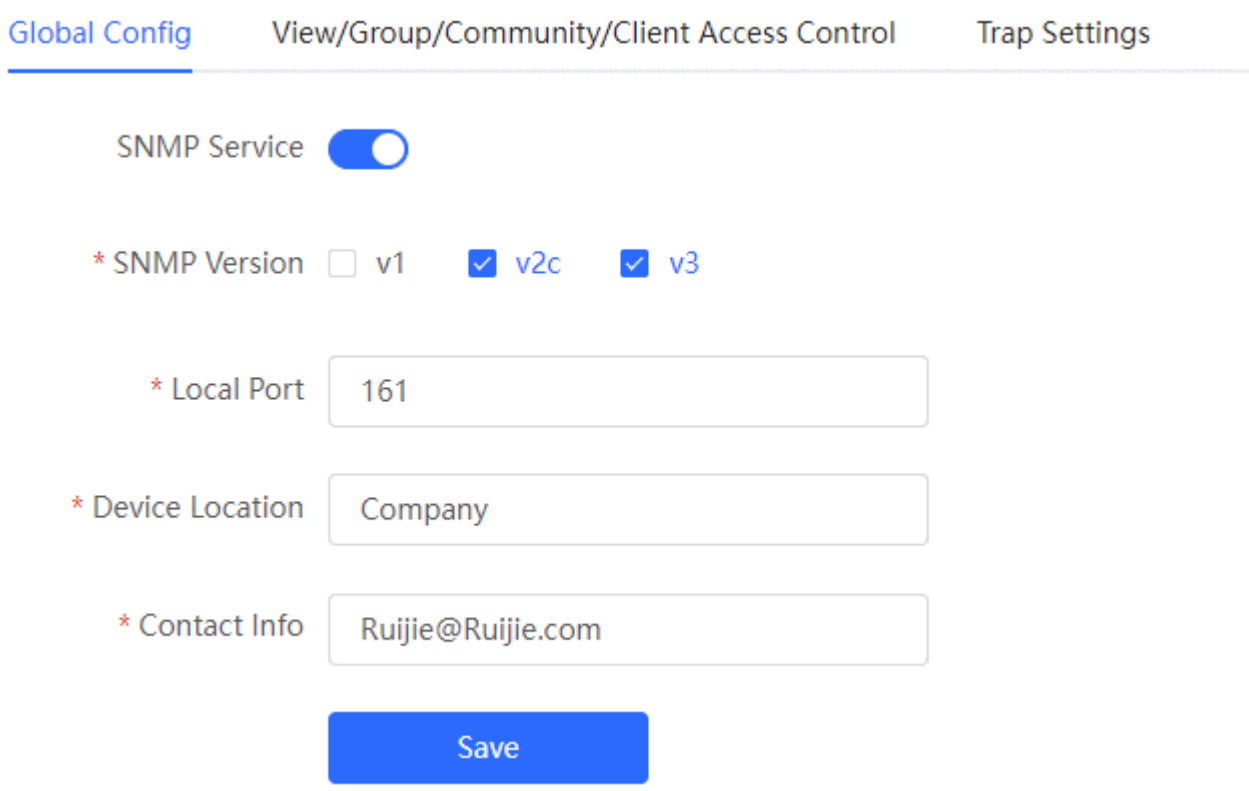


Table 4-1 **Global Configuration Description Table**

Parameter	Parameter
SNMP Service	Whether the SNMP service is enabled or not.
SNMP Protocol Version	SNMP protocol version number includes v1 version, v2c version, and v3 version.
Local Port	[1, 65535]
Device Location	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.
Contact Information	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.

(3) Click <Save>.

After enabling the SNMP service takes effect, click <Save> to make basic configurations such as SNMP protocol version number take effect .

15.4.3 View/Group/Community/Client Access Control

1. View/Group/Community/Client Access Control

MIB (Management Information Base) can be regarded as a database of different status information and performance data of network devices containing a large number of OID (Object Identifiers), which are used to identify different status information and performance data of network devices in snmp .

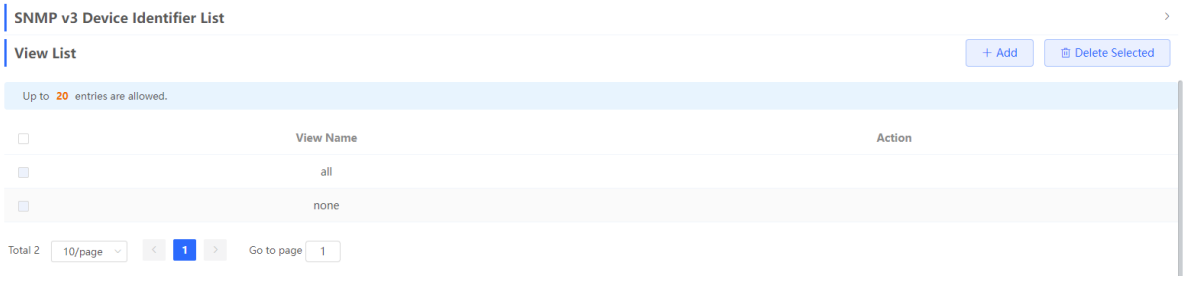
The role of views in snmp is to limit the node range that management systems can access in MIBs so as to improve network management security and reliability. Views are an indispensable part of SNMP management that needs to be configured and customized according to specific management requirements rements.

Views can define multiple subtrees according to requirements limiting the MIB nodes that management systems can only access within these subtrees while unauthorized MIB nodes cannot be accessed by unauthenticated system administrators thus protecting network device security. At the same time views also optimize network management efficiency improving response speed for managing systems.

Configuration Steps:

[Network-wide Management - Page Wizard] System >> SNMP >> View/Group/Community/Client Access Control >> View List

(1) Click <Add> to create a view.



(2) Configure the basic information of the view .

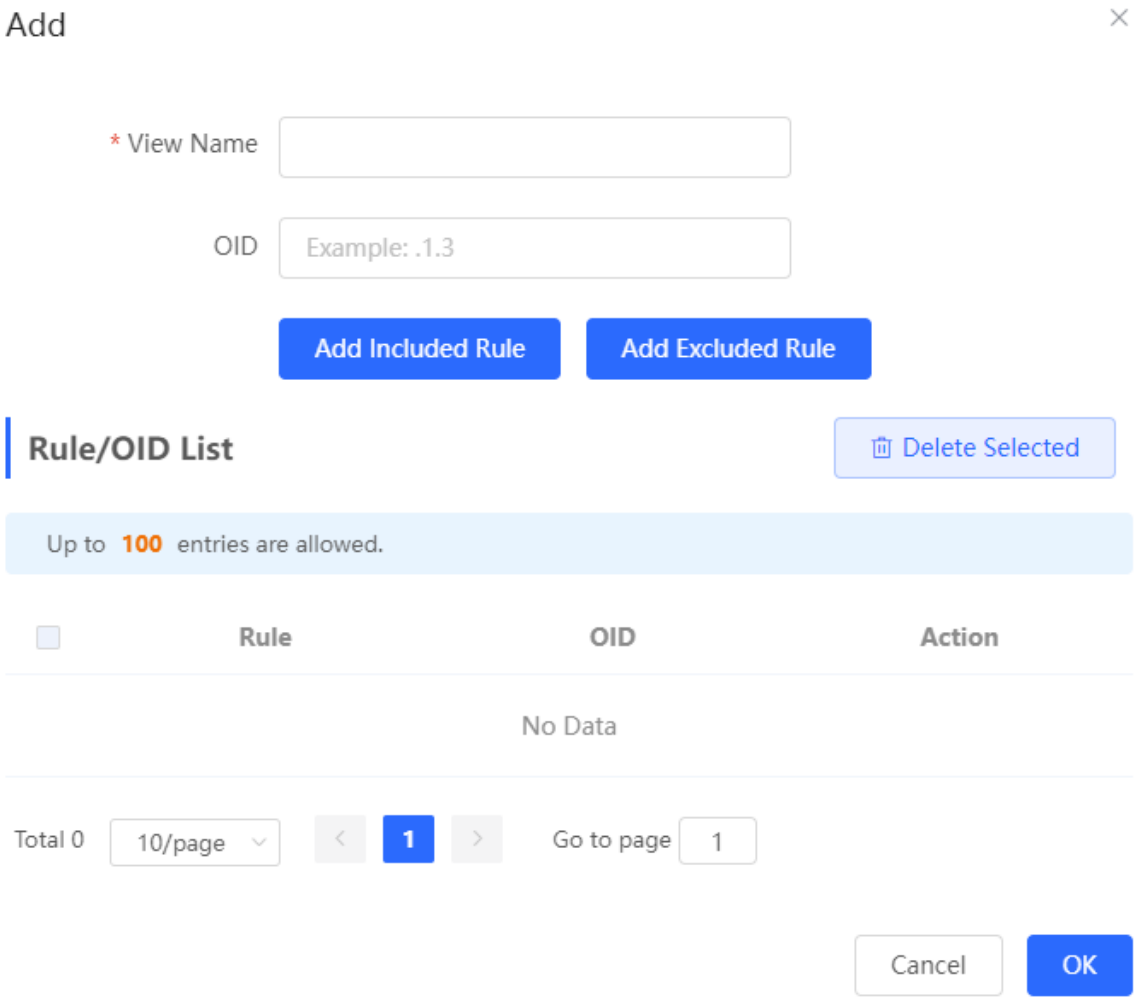


Table 4-2 **View configuration information description table**

parameter	illustrate
View Name	The name used to identify the view. The length is 1 to 32 characters, and cannot contain Chinese

parameter	illustrate
	and full-width characters.
OIDs	Define the range of OIDs included in the view, which can be a single OID or a subtree of OIDs
Add Included Rule or Excluded Rule Add Included Rule Add Excluded Rule	Divided into inclusion rules and exclusion rules ● Include rules allow access only to OIDs within the OID range . Click <Add Inclusion Rule> to set up this type of view. ● Exclusion rules allow access to all OIDs except the OID range . Click <Add Exclusion Rule> to set up this type of view.

Notice

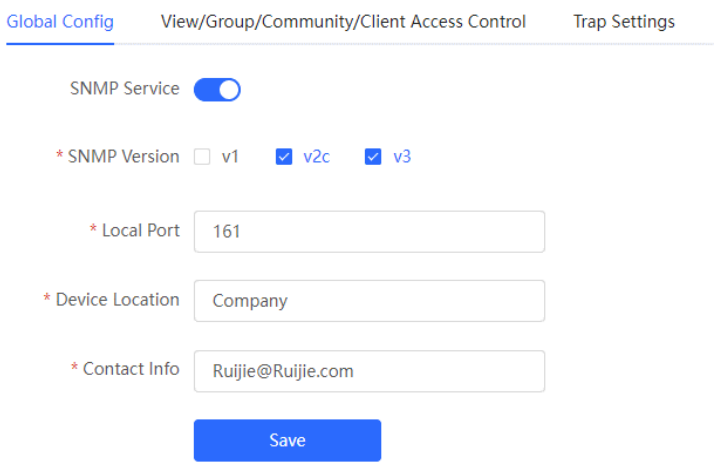
For the created view, add at least one OID rule , otherwise a warning message will appear .

(3) Click <OK> .

5. v1 /v2c user configuration

- Introduction

  When the SNMP protocol version is set to v1/v2c, user configuration needs to be completed.



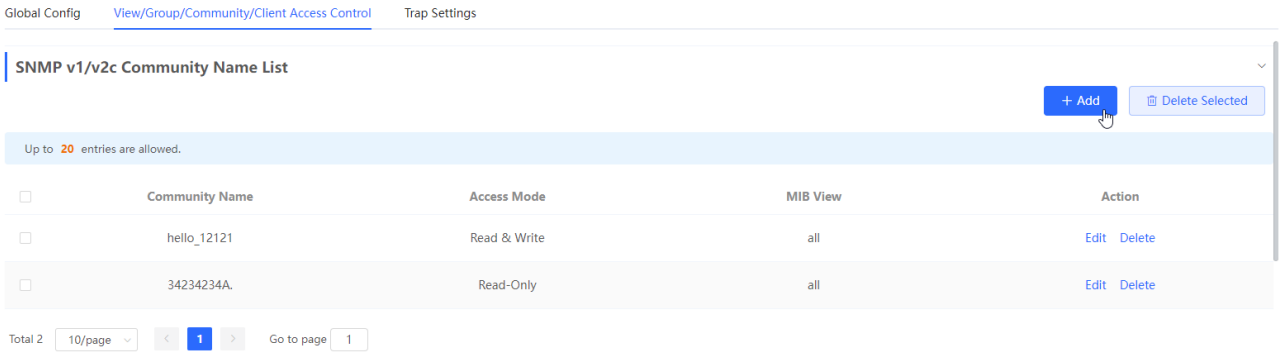
illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

  [Entire Network Management-Page Wizard]System>>SNMP>> View/Group/Community/Client Access Control

(1) In the " SNMP v1/v2c Community Name List " area, click <Add>.



(2) Create v1/v2c users.

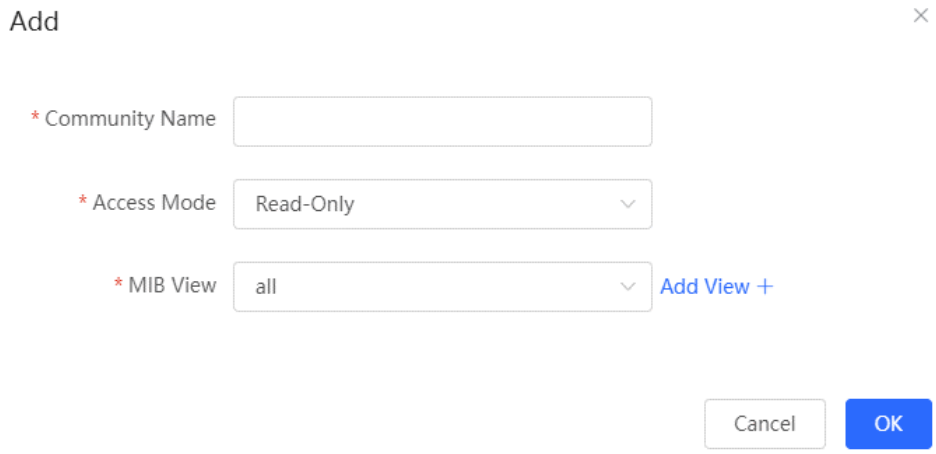


Table 4-1 **v1 / v2c user information description table**

parameter	**illustrate**
Community Name	at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private

parameter	illustrate
	Do not contain question marks, spaces and Chinese
Access Mode	Access rights of the community name (read-only , read-write) Read & Write Read-Only
MIB View	The options in the drop-down box are configured views (default views all , none)

Notice

- Among v1/v2c users, the community name cannot be repeated .
- Click <Add View> to add a view .

6. v3 group configuration

- Introduction

  SNMPv3 introduces the concept of grouping for better security and access control. A group is a group of SNMP users with the same security policy and access control settings. Using SNMPv3 , multiple groups can be configured, each group can have its own security policy and access control settings, and each group can also have one or more users.

- prerequisite

  When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.

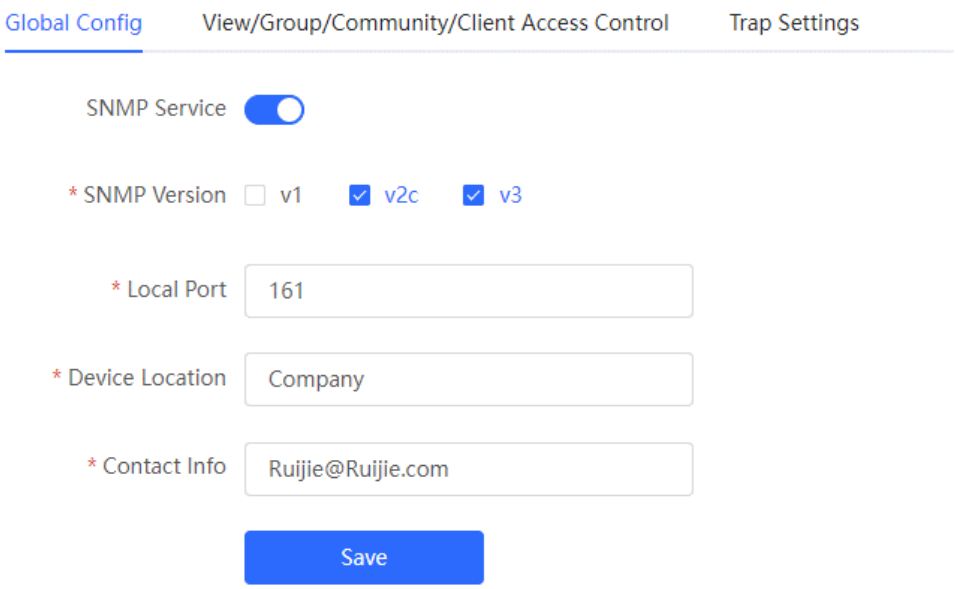
illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

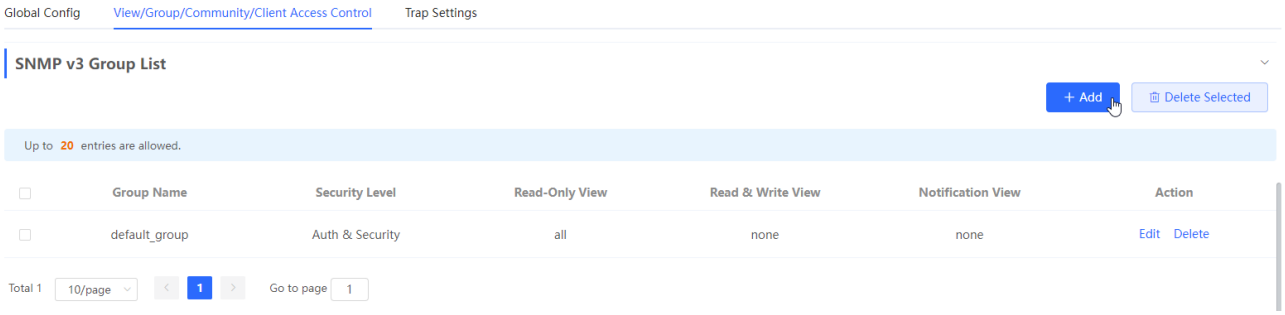
- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control.

(1) Click <Add> in the " SNMP v3 Group List " area to create a v3 group .



(2) Set v 3 groups of related parameters.



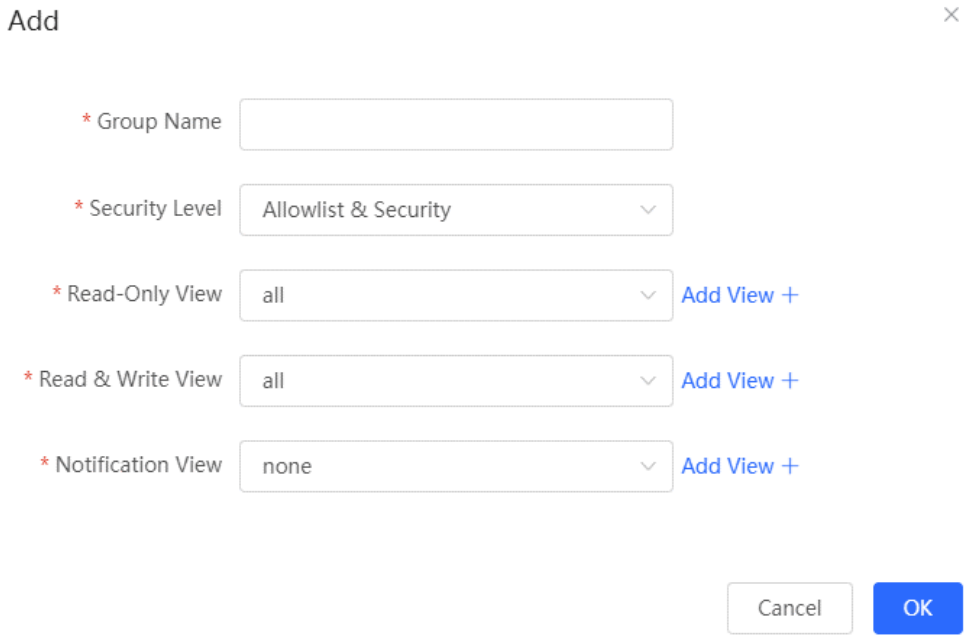


Table 4-1 **V3 group configuration parameters**

parameter	illustrate
Group Name	rule group name 1-32 characters, a single Chinese accounted for three characters Cannot contain Chinese, full-width characters, question marks and spaces
Security Level	The minimum security level of the rule group (**Auth & Security** Auth & Open Allowlist & Security authentication with encryption, authentication without encryption, no authentication encryption)
Read-Only View	The options in the drop-down box are configured views (default views all , none)
Read & Write View	The options in the drop-down box are configured views (default views all , none)
Notification View	The options in the drop-down box are configured views (default views all , none)

⚠ Notice

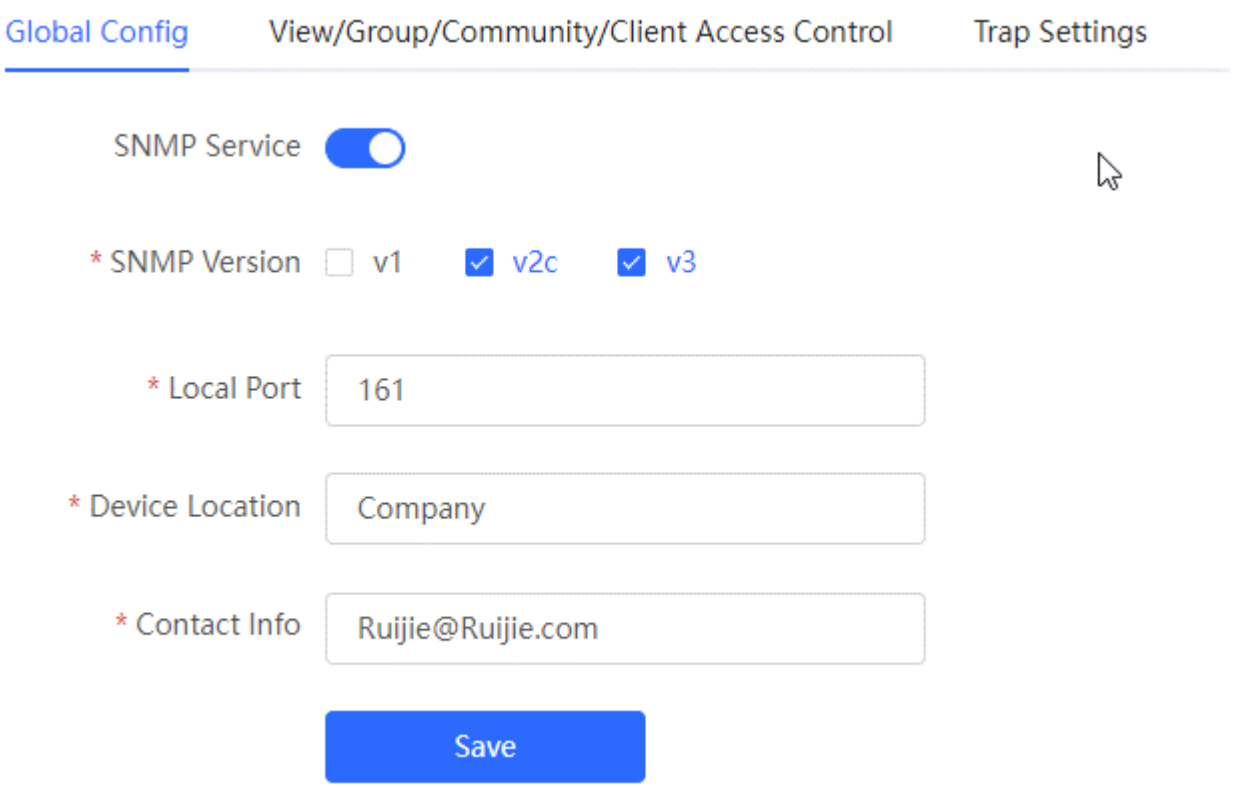
- Groups limit the minimum security level, read and write permissions and scope of users in the group.
- The group name cannot be repeated . If you need to add a view, click < Add View >.

(3) Click <OK> .

7. v 3 user configuration

- Introduction
- prerequisite

When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.



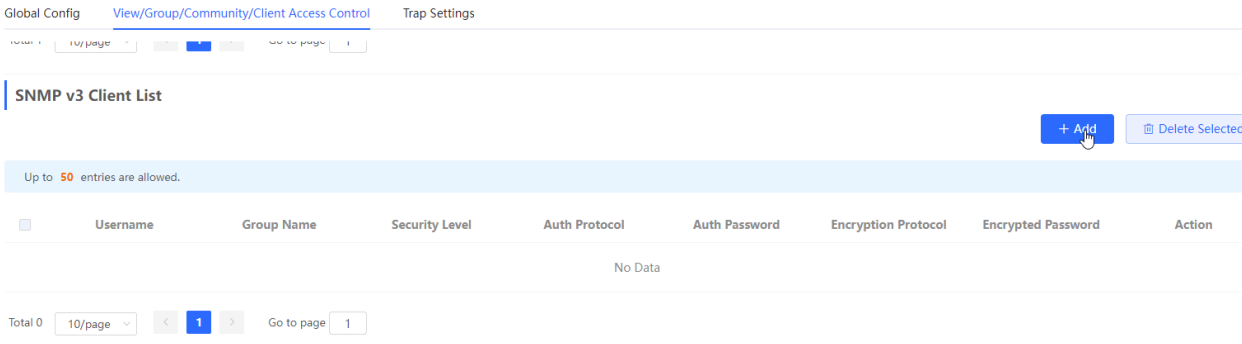
illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control >>.

(1) In the " SNMP v3 Client List " area, click <Add> to create a v3 user .



(2) Set v3 user related parameters.

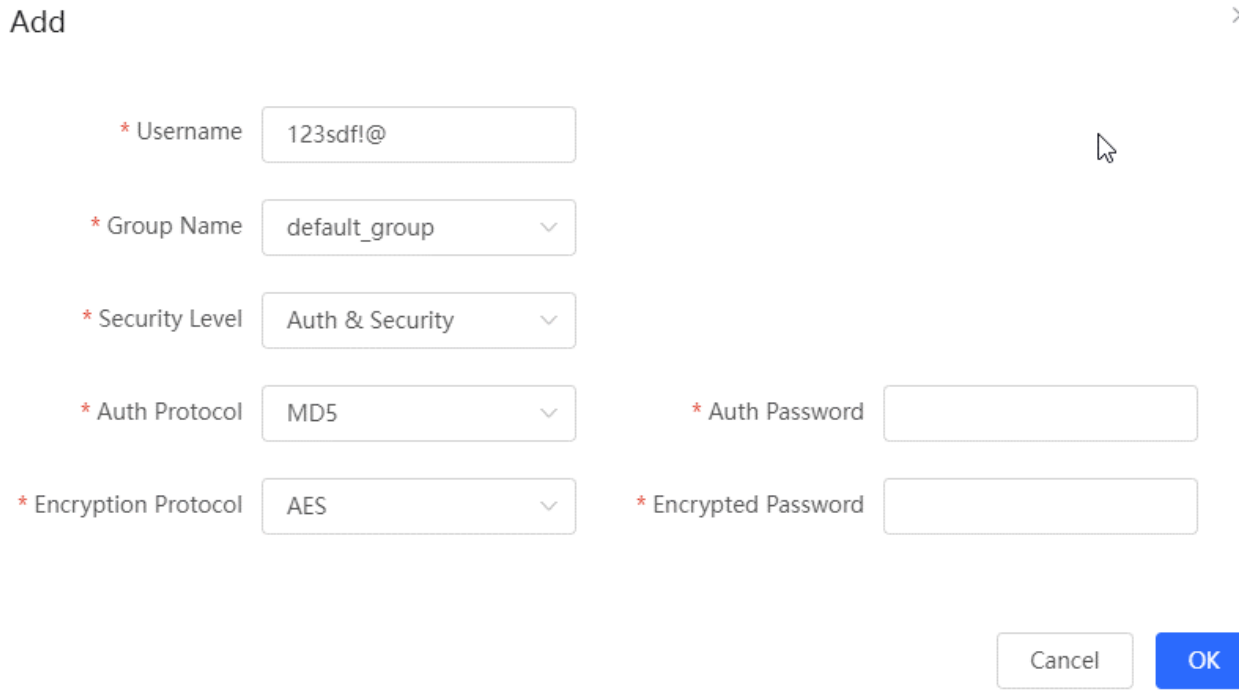


Table 4-1 **v3 user configuration parameters**

parameter	**illustrate**
Username	username at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Does not contain question marks, spaces and Chinese
Group Name	user's group
Security Level	User security level (authentication and encryption, authentication without encryption, no authentication and encryption)
Auth Protocol , Auth Password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces , and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters . Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".

parameter	illustrate
Encryption Protocol , Encrypted Password	Encryption protocols include: DES/AES/AES192/AES256 Encrypted password : the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format, containing at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.

⚠ Notice

- The security level of the v3 user must be greater than or equal to the security level of this group.
- There are three security levels. For authentication and encryption, you need to configure the authentication protocol, authentication password, encryption protocol, and encryption password. For authentication without encryption, you only need to configure the authentication protocol and encryption protocol. Without authentication and encryption, no configuration is required.

15.4.4 Typical Configuration Examples of SNMP Service

3. v2c version SNMP service configuration

- scenes to be used

  The user only needs to monitor the information of the device, and does not need to set and issue, and uses the v2c version to monitor the data information of nodes such as 1.3.6.1.2.1.1 through the third-party software.

- configuration list

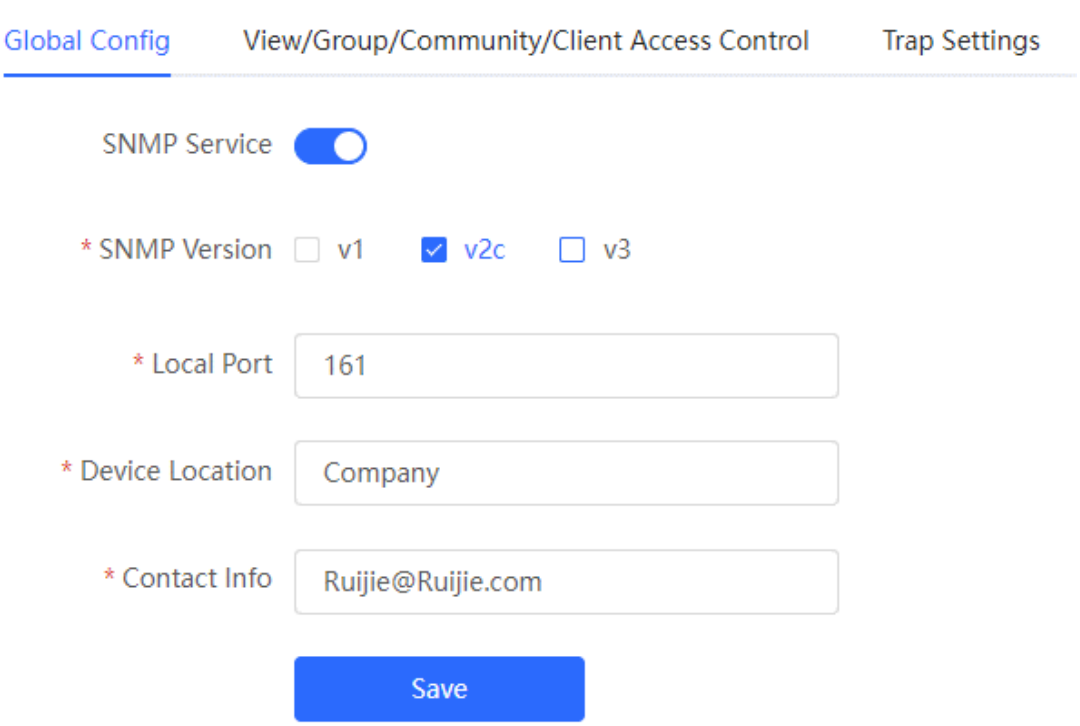
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

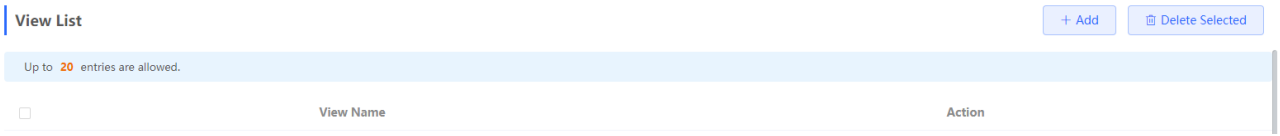
description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1.1 , custom view named " system "
use version number	v2c version The custom community name is " public ", and the default port number is 161
Read and write permissions	Read permission

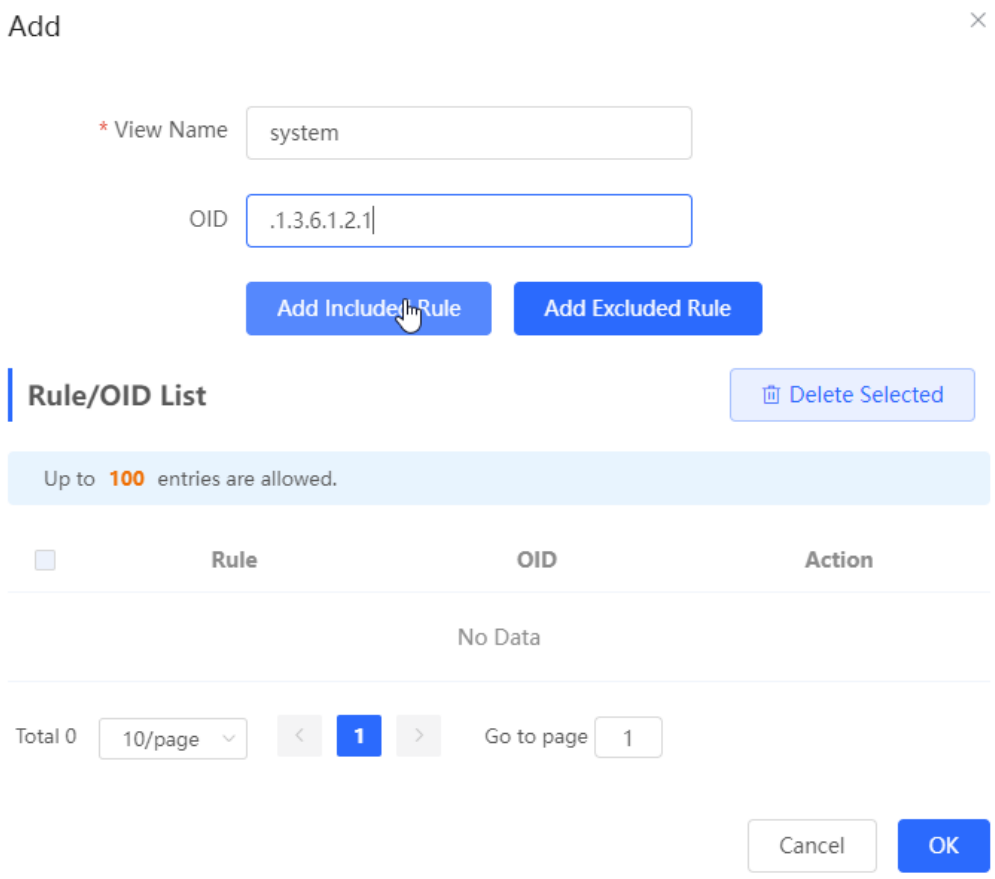
- configuration steps

(5) On the global configuration interface, select the v2c version, and leave other settings as default. After the operation is complete, click <Save> .

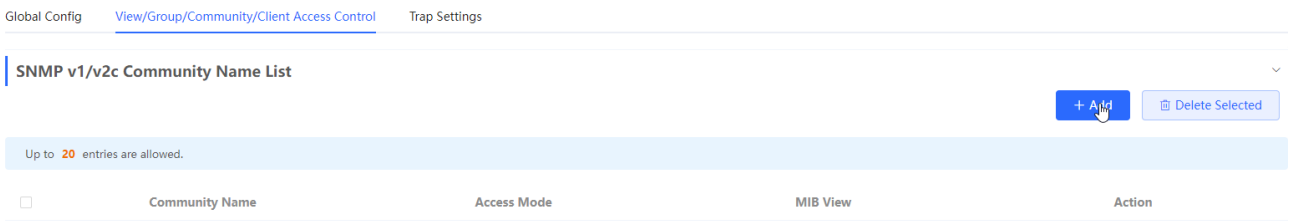


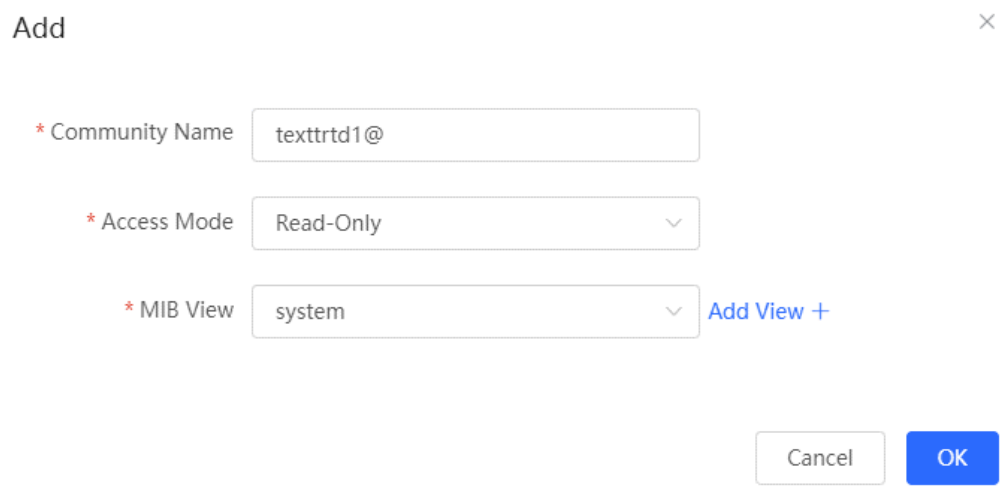
(2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and O ID in the pop-up window and click <Add inclusion rule>, and click <OK> after the operation is complete .





(3) view /group/group/user access control interface, 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.





4. v 3 version SNMP service configuration

- scenes to be used

  Users need to monitor and control the equipment, and use the v3 version of the third-party software to monitor and send data to the public node (1.3.6.1.2.1) node. The security level of the v3 version adopts authentication and encryption.

- configuration list

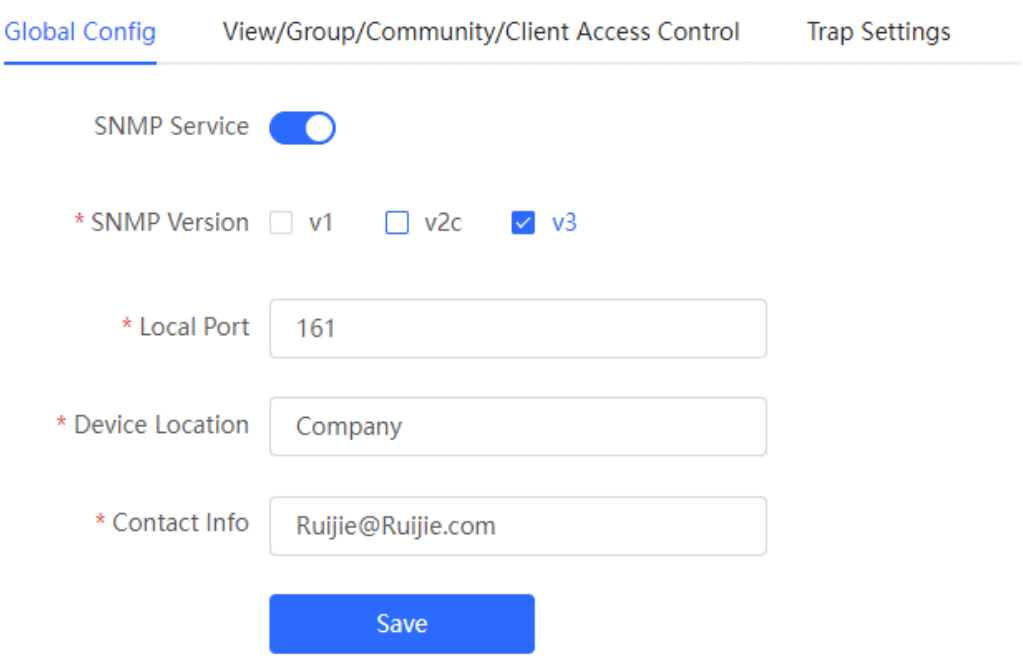
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

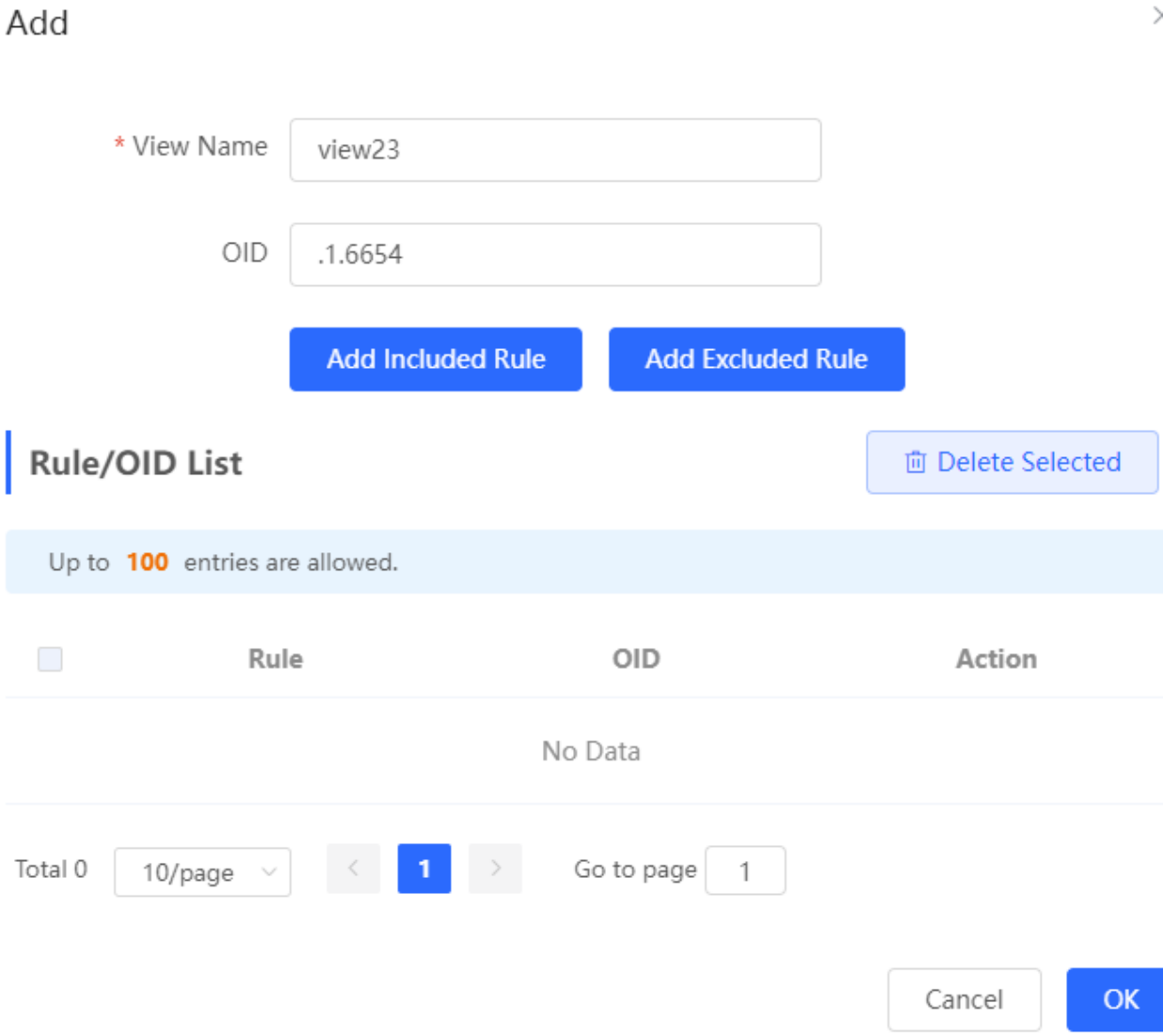
description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1 and custom view is named " public_view "
group configuration	Group name: group Security level: authenticated and encrypted Readable view select " public_view " Writable view select " public_view " Notification view select " none "
v3 user configuration	Username: v3_user Group name: group Security level: authenticated and encrypted Authentication protocol / authentication password: MD5/Ruijie123 Encryption protocol / encryption password: AES/ Ruijie123
use version number	v3 version, default port 161

- configuration steps

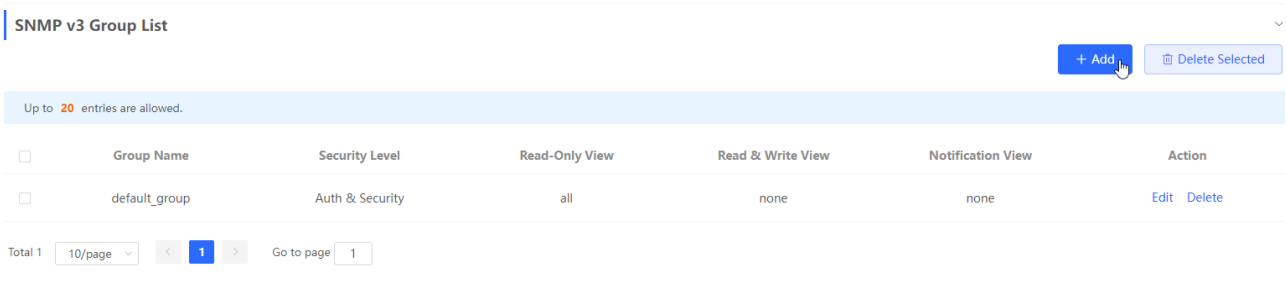
(6) Select the v3 version on the global configuration interface , change the port to 161, and set other settings to default. After the operation is complete, click <Save>.

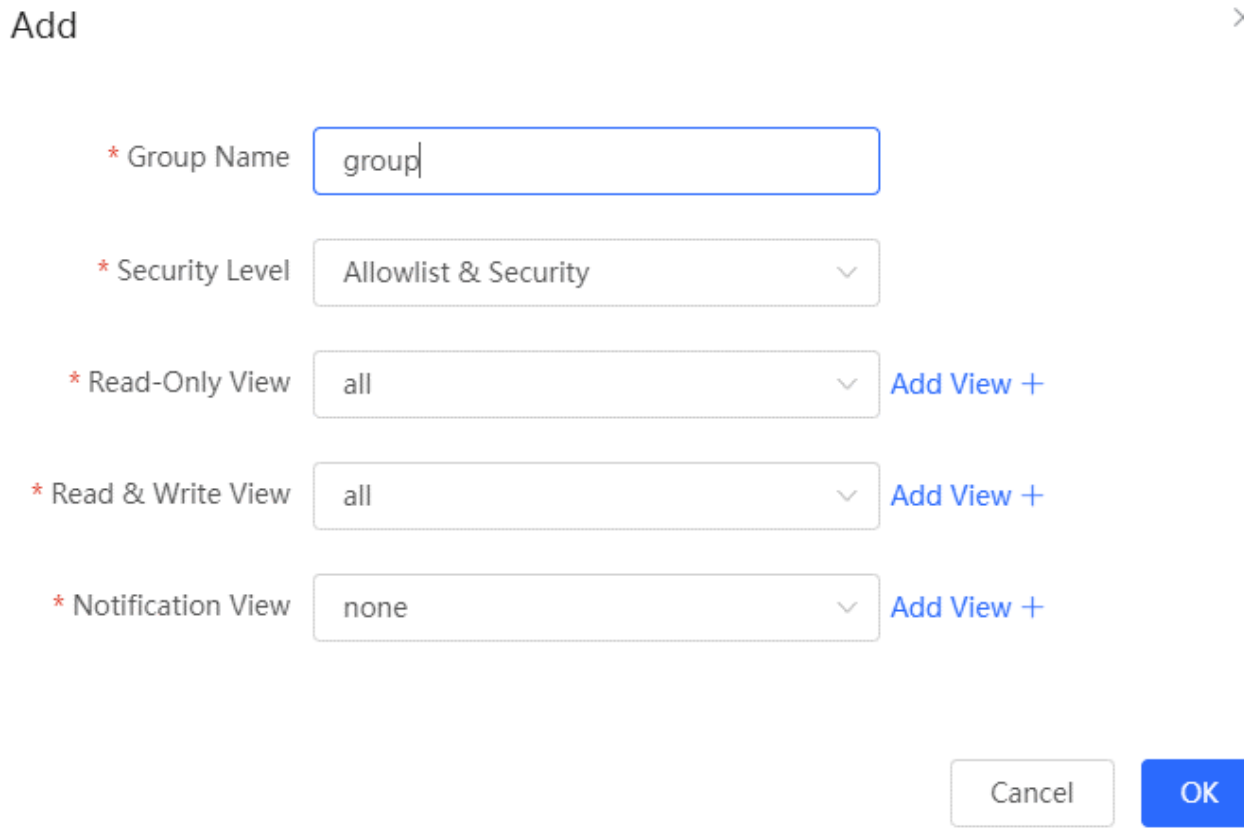


(2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and OID in the pop-up window, click <Add Inclusion Rule>, and click <OK> after the operation is complete.

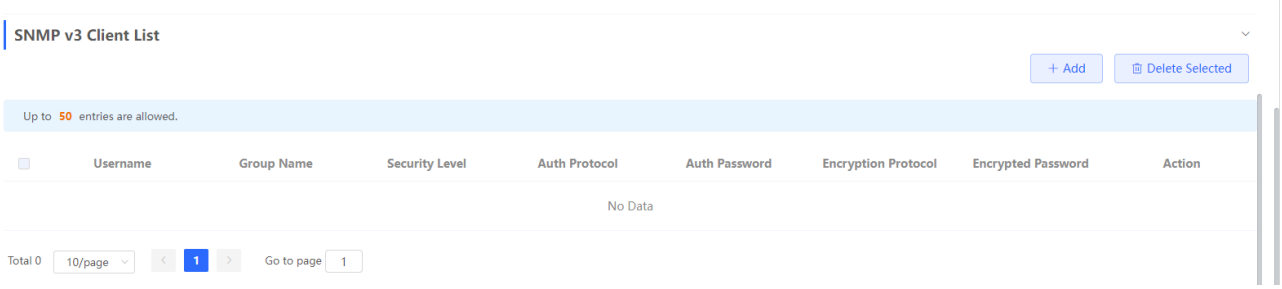


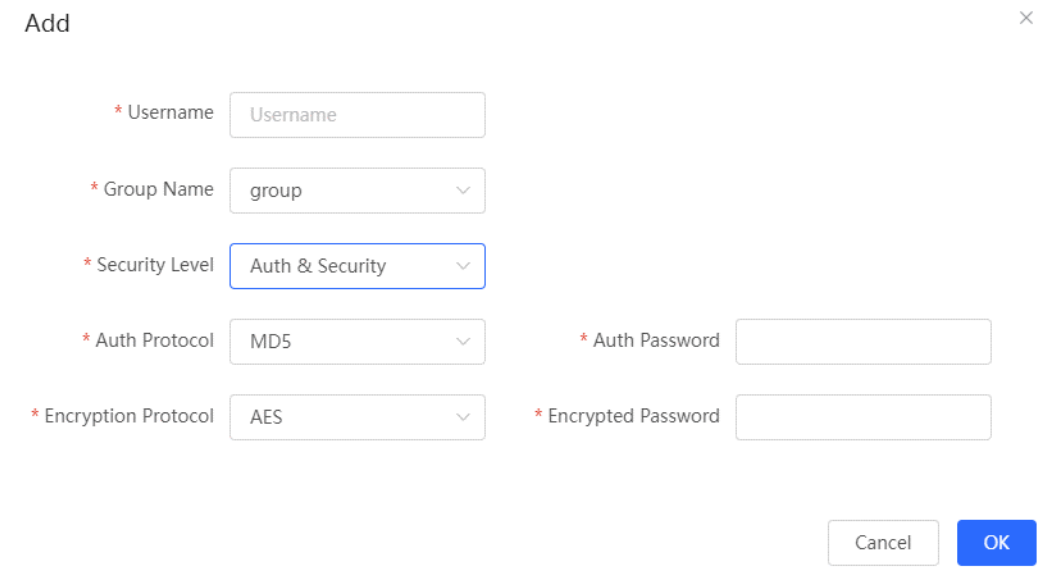
(3) Click <Add> in the SNMP v3 group list, fill in the group name and security level in the pop-up window , the user has read and write permissions, select " public _view " for the readable view and read and write view , and set the notification view to none. After the operation is complete, click <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





(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>.





15.4.5 trap service configuration

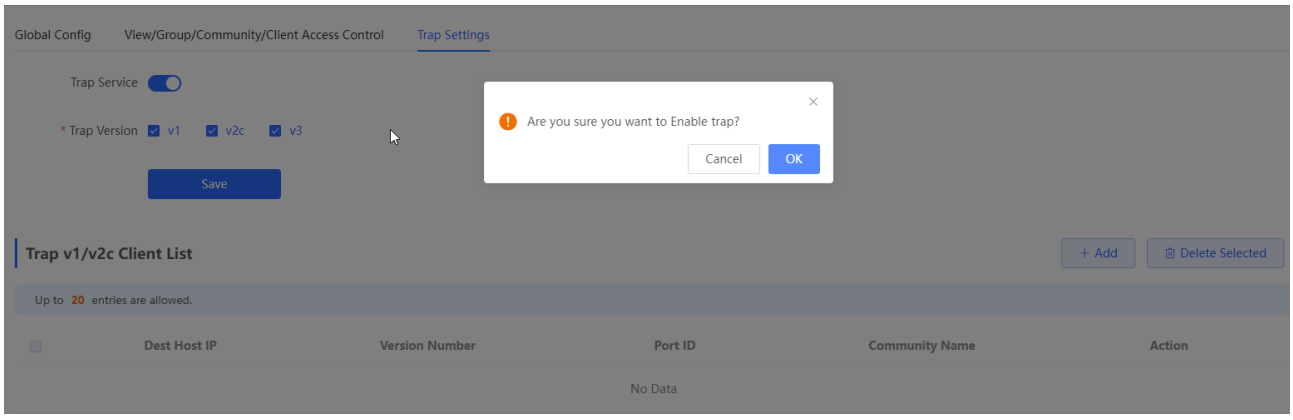
trap is a notification mechanism of the SNMP (Simple Network Management Protocol) protocol, which is used to report the status and events of network devices to managers, including device status reports, fault reports, performance reports, configuration reports and security management. Trap can provide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

4. trap open settings

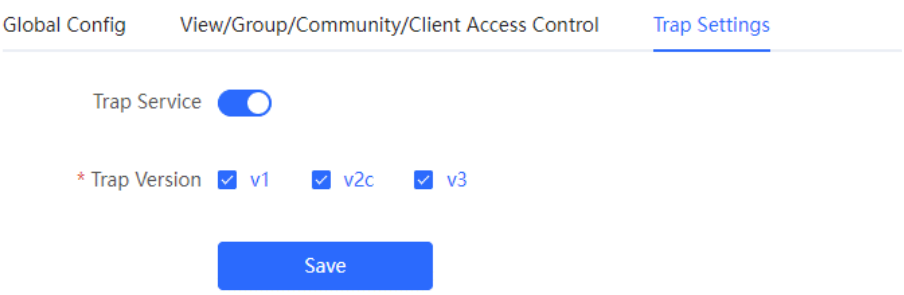
Enable the trap service and select the effective trap protocol version, including v1, v2c , and v3 .

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

(1) Enable the trap service switch.



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



(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.

5. 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 in the network in time and take corresponding measures.

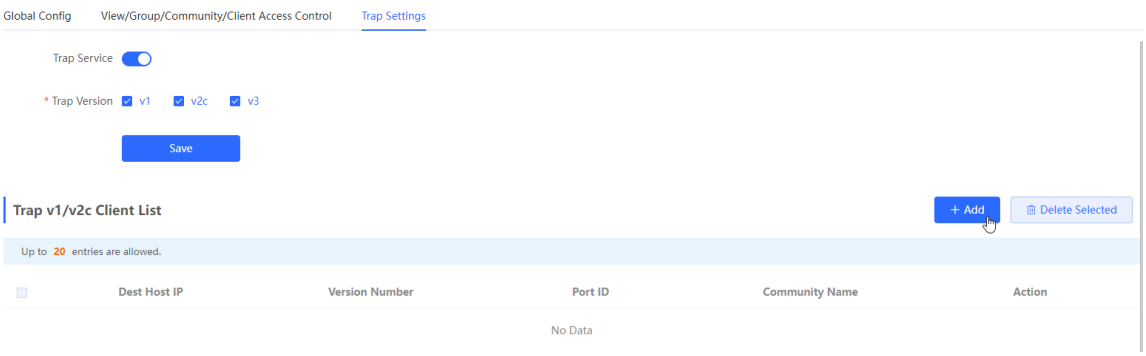
- prerequisite

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

- configuration operation

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

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



(2) Configure trap v1v2c user-related parameters.

set up

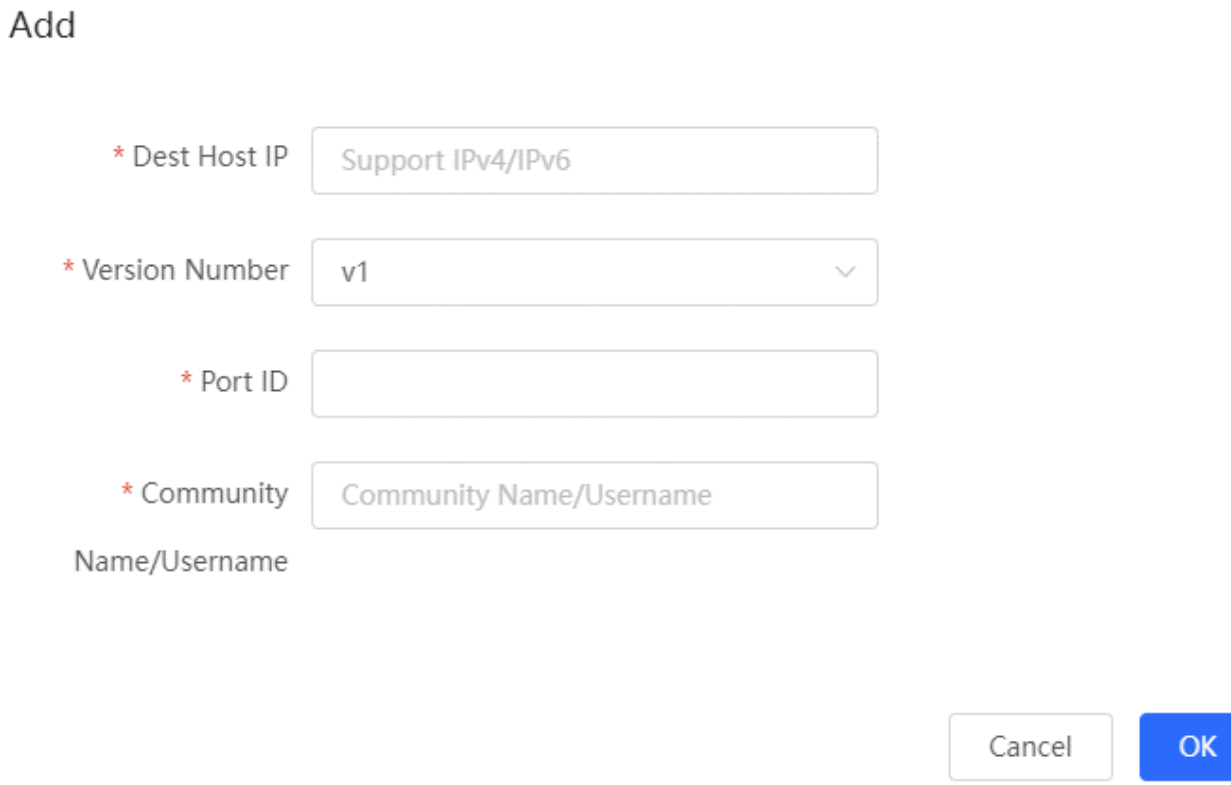


Table 4-1 **t rap v1/v2c user information description table**

parameter	**illustrate**
destination ip	Trap peer device IP, support IPv4 / IPv6 address
version number	Trap version number, including v1|v2c
The port number	trap peer device port [1, 65535]
Group Name/User Name	The community name of the trap user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese

Notice

- IP address of trap v1/v2c /v3 users cannot be repeated .
- Trap v1/v2c user names cannot be repeated.

(3) Click <OK>.

6. 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.

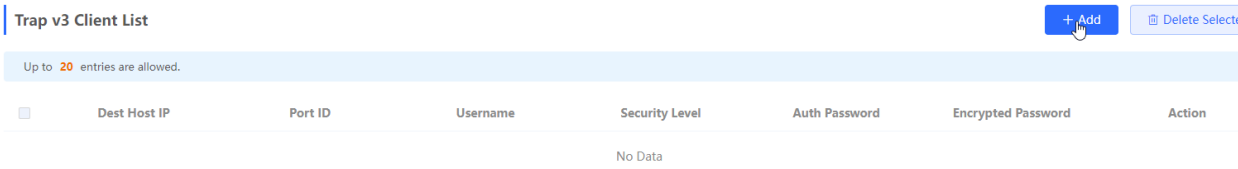
- prerequisite

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

- configuration steps

  [Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

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



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

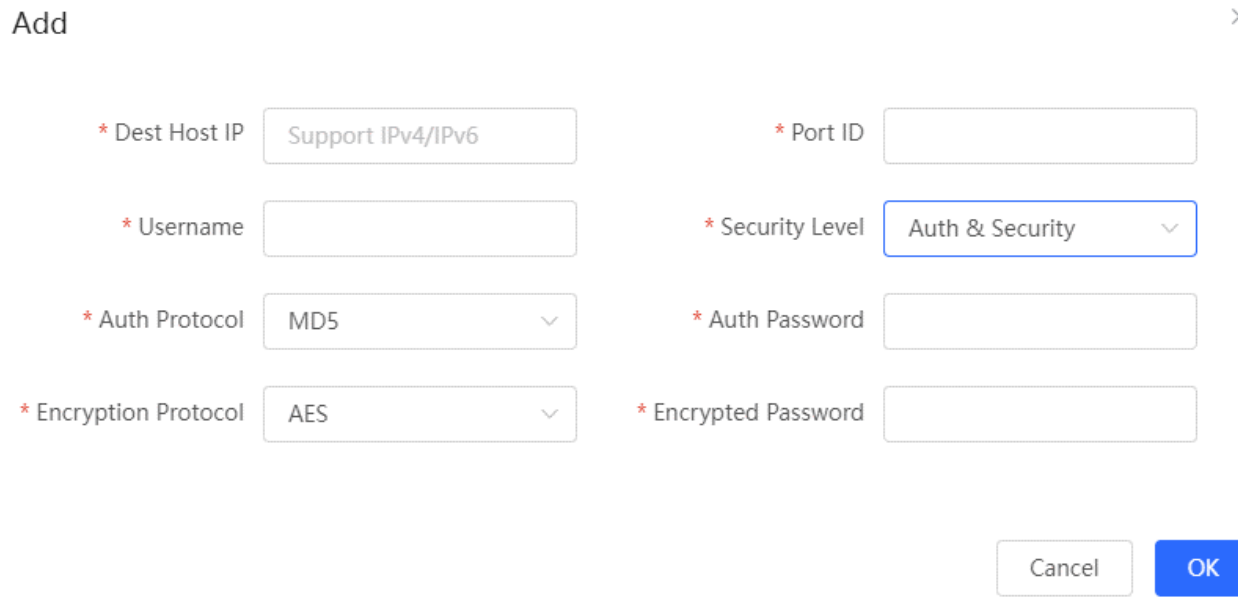


Table 4-1 **trap v3 user information description table**

parameter	illustrate
target host ip	trap peer device IP , support IPv4/IPv6 address
The port number	trap peer device port [1, 65535]
username	username of the trap v3 user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Security Level	Trap user security level, including three levels of authentication and encryption, authentication and encryption, and authentication and no encryption
Authentication protocol, authentication password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~ 31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces, and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".
encryption protocol, encryption password	Encryption protocols include: DES/AES/AES192/AES256 Encrypted password: the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format, containing at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.

⚠ Notice

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

15.4.6 Typical configuration examples of the trap service

3. v2c version trap configuration

- scenes to be used

  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 list

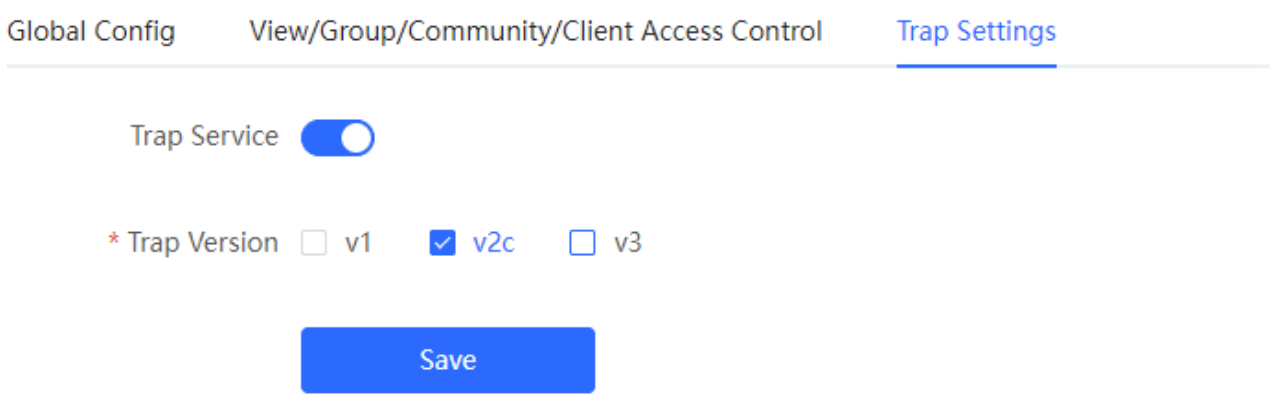
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

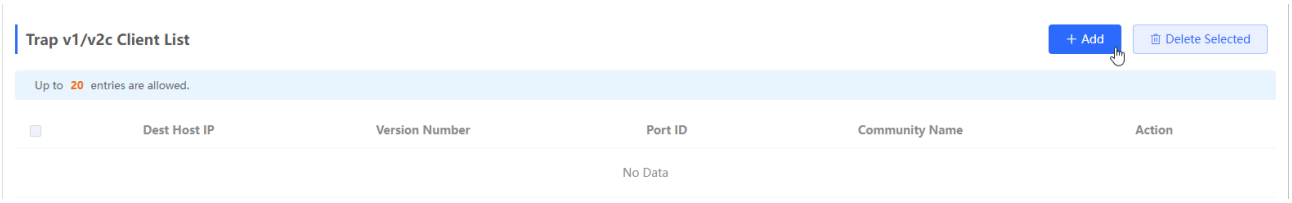
description item	illustrate
IP and port number	The target host IP is "192.168.110.85" , and the port number is "166" .
use version number	Select v2 version
Group Name / User Name	Trap_public

- configuration steps

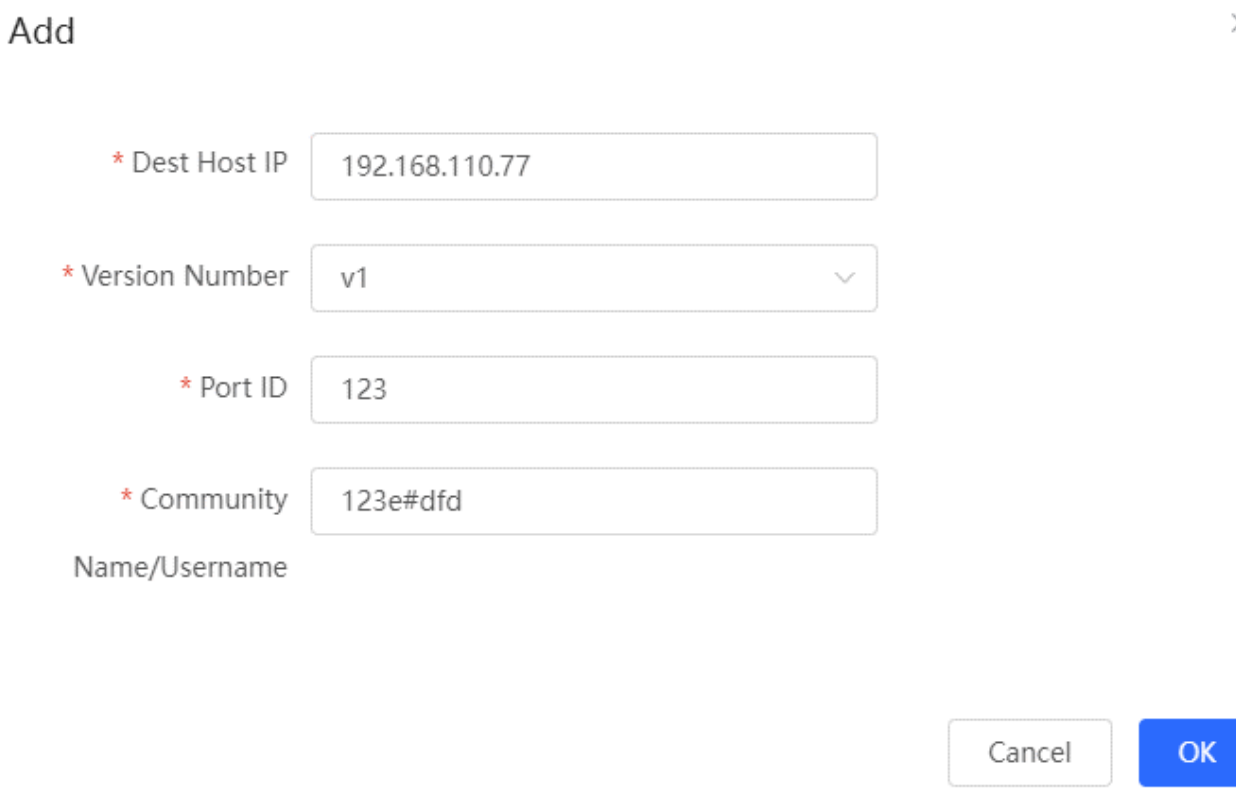
(7) Select the v2c version on the trap setting interface , click <Save> ,



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



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



4. V3 version trap configuration

- scenes to be used

  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 list

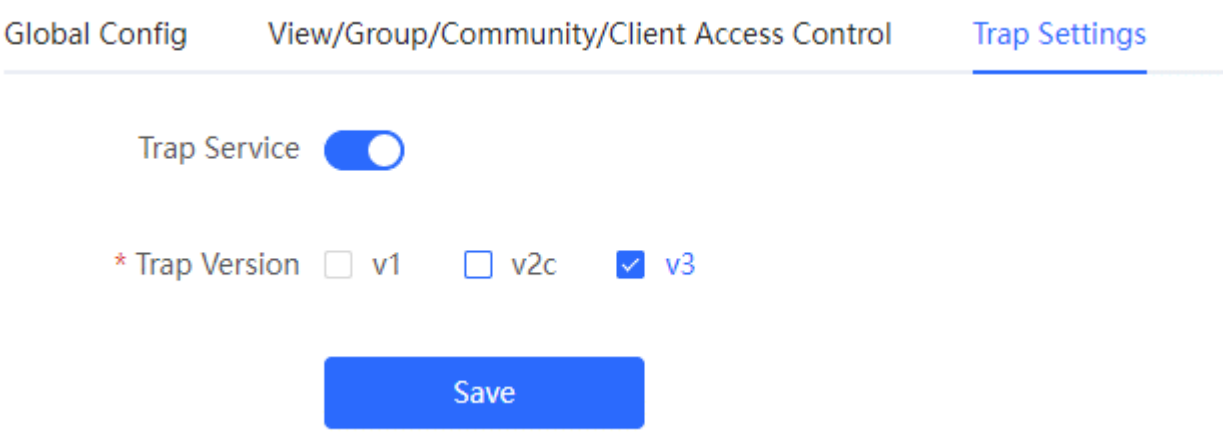
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 4-1 **User Requirements Description Form**

description item	illustrate
IP and port number	The target host IP is "192.168.110.87" , and the port number is "167" .
Use version number, username	Select the v3 version, the user name is "trapv3_public"
Authentication Protocol / Encryption Protocol Encryption Protocol / Encryption Cipher	Authentication protocol / authentication password: MD5/Ruijie123 Encryption protocol / encryption password: AES/ Ruijie123

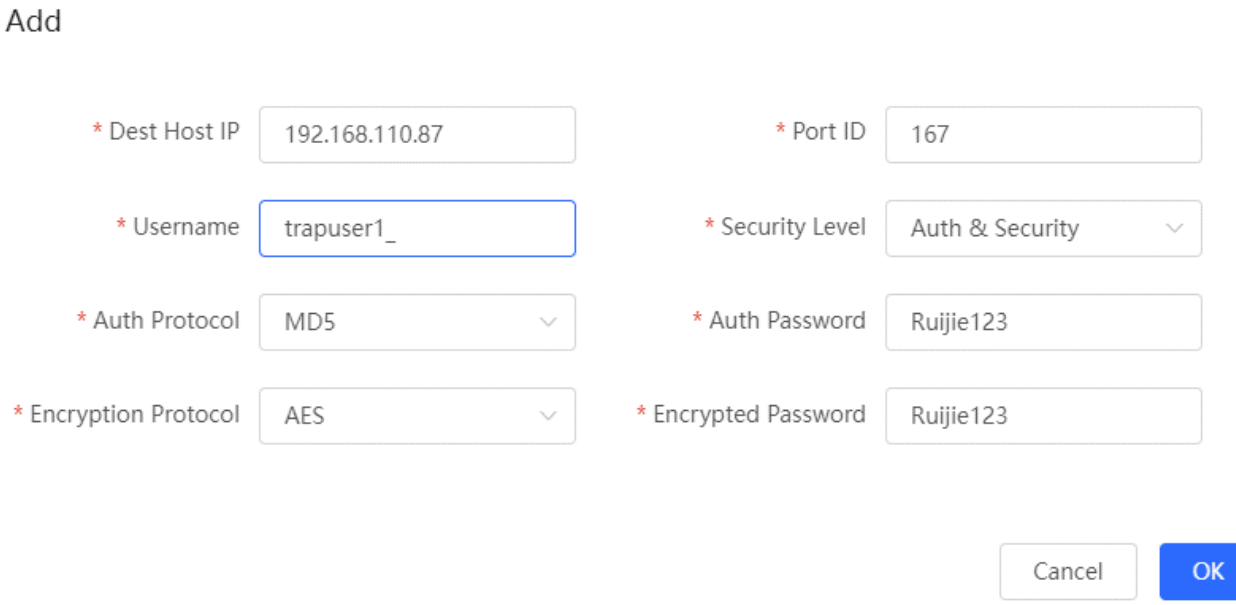
- configuration steps

(8) Select the v3 version on the trap setting interface , and click <Save> .



(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.

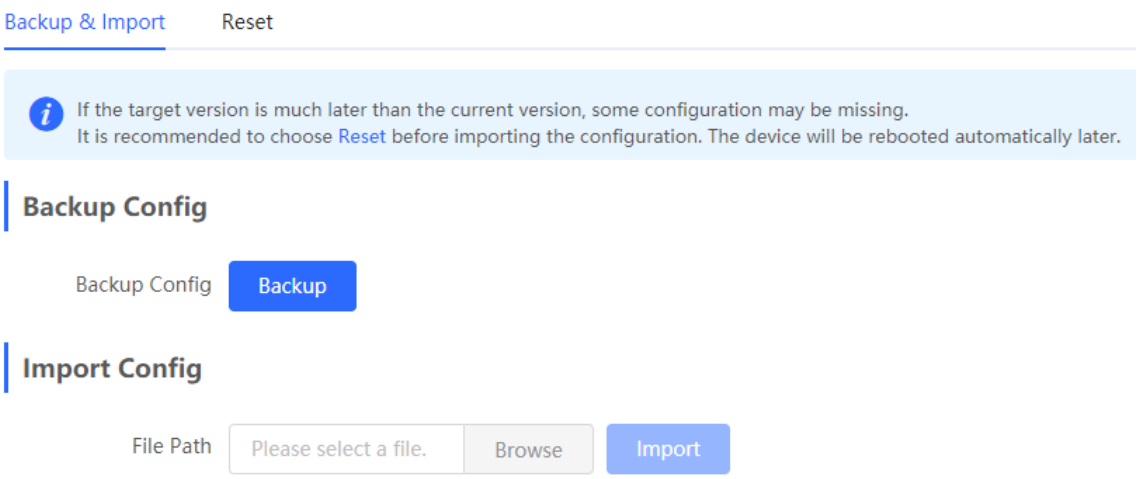


15.5 Configuration Backup and Import

Choose **System** > **Management** > **Backup & Import** .

Configure backup: Click **Backup** to generate the backup configuration and download it locally.

Configure import: Click **Browse** , select a backup configuration file locally, and click **Import** to apply the configuration specified by the file to the device After importing the configuration, the device will restart.

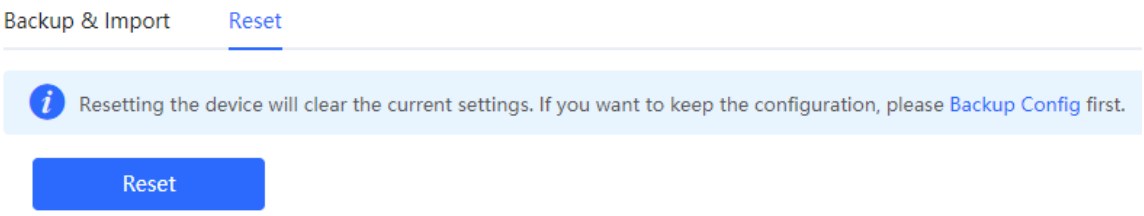


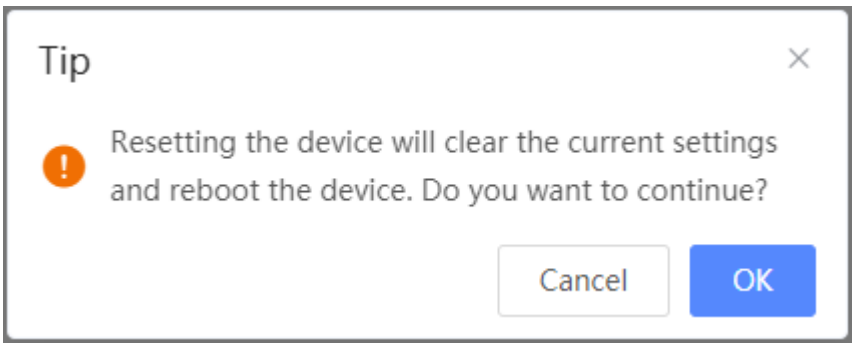
15.6 Reset

15.6.1 Resetting the Device

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

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





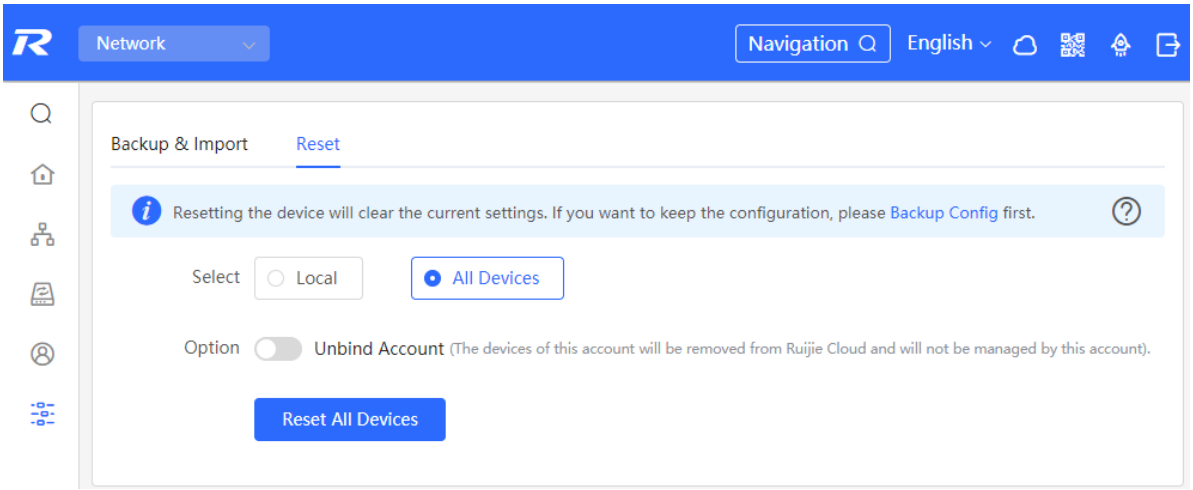
Caution

Resetting the device will clear current settings and reboot the device. If a useful configuration exists in the current system, you can export the current configuration (see 10.4) before restoring the factory settings. Exercise caution when performing this operation.

15.6.2 Resetting the Devices in the Network

Choose **Network** > **System** > **Management** > **Reset**.

Select **All Devices** and choose whether to **Unbind Account**, click **Reset All Devices** and all devices in the current network will be restored to their factory settings.



Caution

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

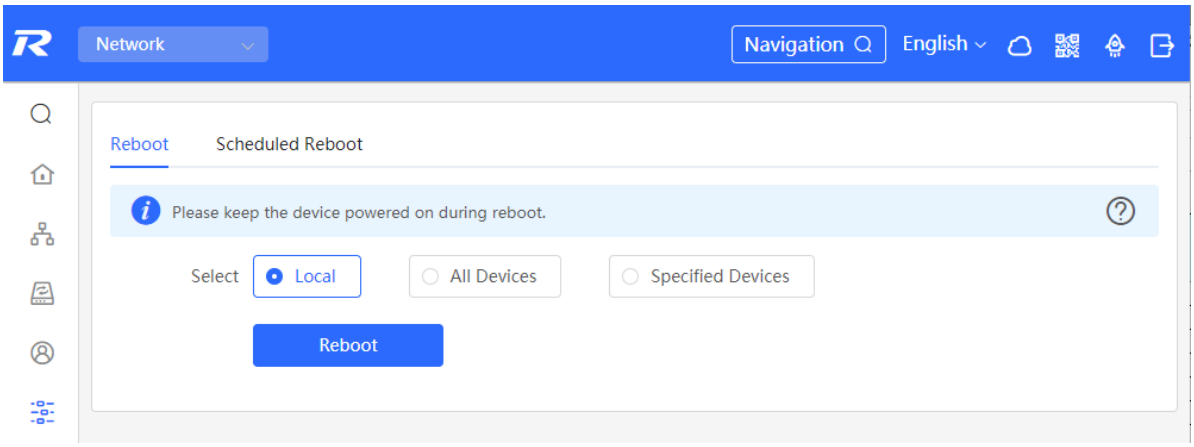
15.7 Rebooting the Device

15.7.1 Rebooting the Device

Choose **Self-Organizing Mode** > **Network** > **System** > **Management** > **Reset**.

Choose **Standalone Mode** > **System** > **Reboot**.

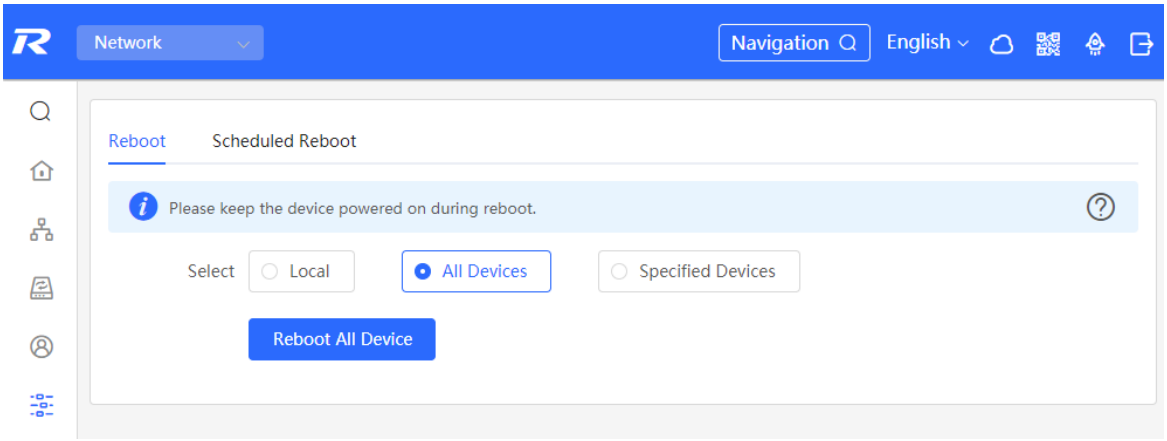
Select **Local** and click **All Devices**. The device will restart. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.



15.7.2 Rebooting the Devices in the Network

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

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



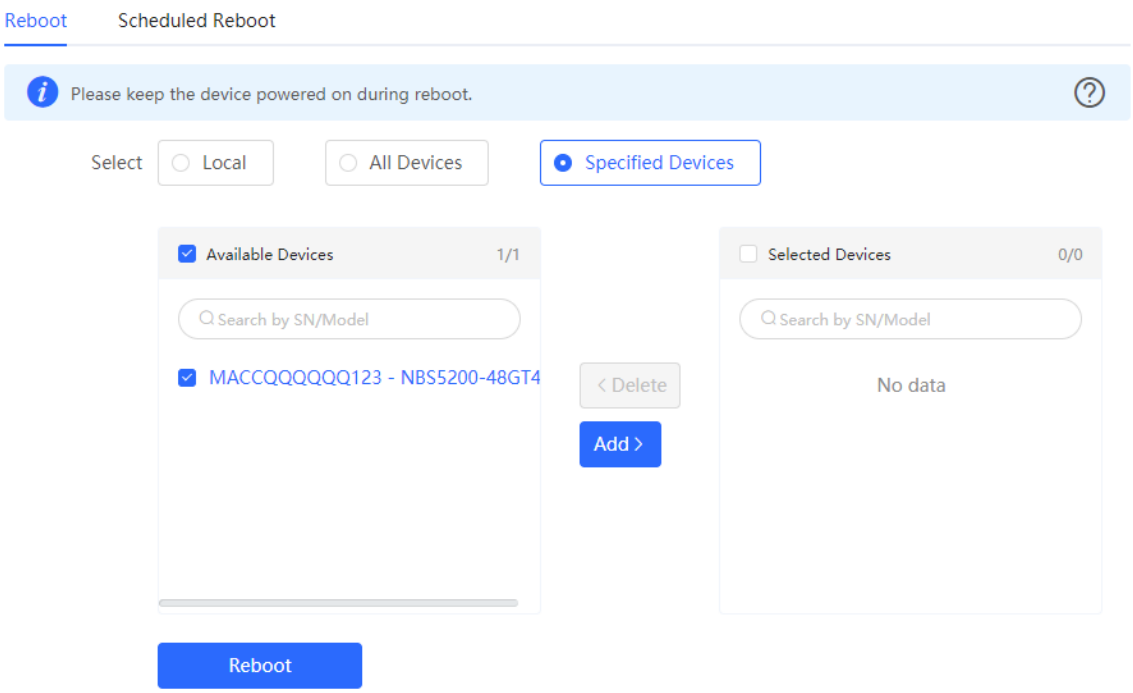
Caution

It will take some time for the network to reboot, please be patient. The network operation will affect the entire network. Therefore, exercise caution when performing this operation.

15.7.3 Rebooting Specified Devices in the Network

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

Click **Specified Devices**, select desired devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.



15.8 Configuring Scheduled Reboot

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

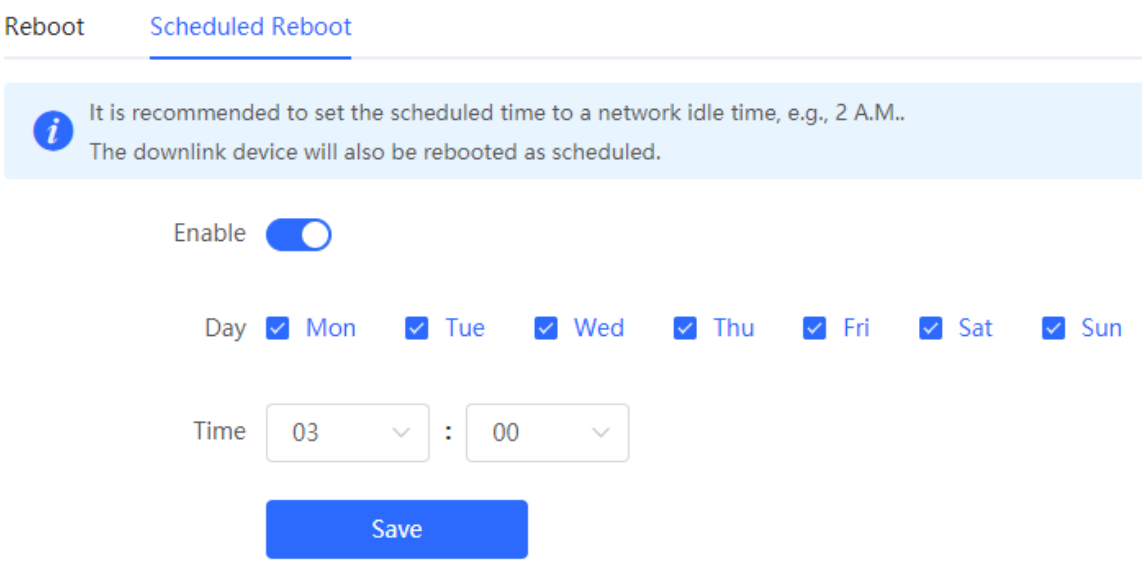
Choose **Self-Organizing Mode** > **Network** > **System**> **Scheduled Reboot**.

Choose **Standalone Mode** > **System** > **Scheduled Reboot**.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.

Caution

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



15.9 Upgrade

Caution

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

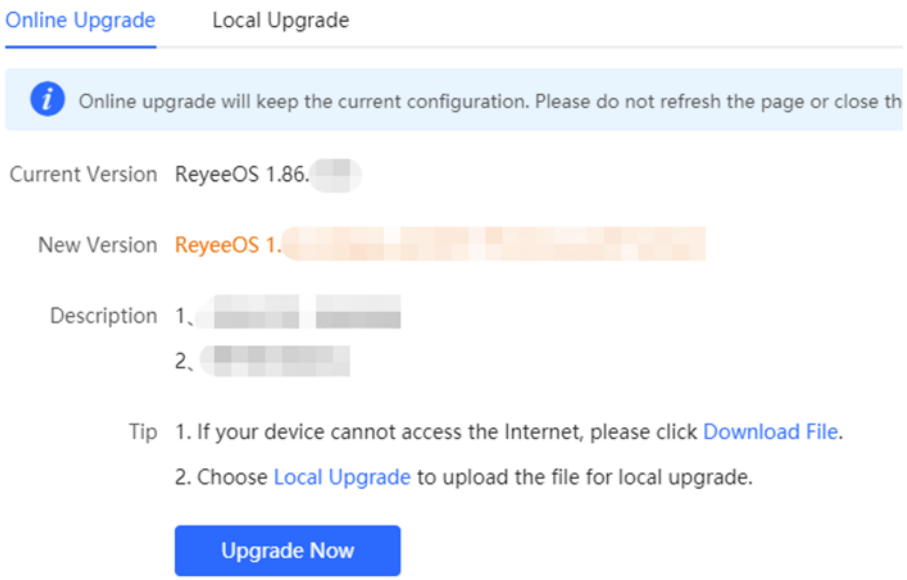
15.9.1 Online Upgrade

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

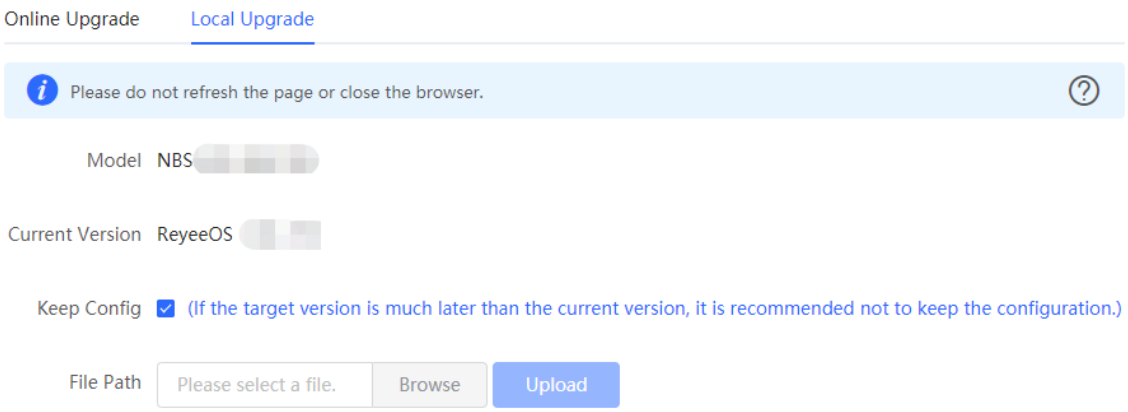
- Online upgrade will retain the current configuration.
- Do not refresh the page or close the browser during the upgrade process. After successful upgrade, you will be redirected to the login page automatically.



15.9.2 Local Upgrade

Choose **Local Device** > **System** > **Upgrade** > **Local Upgrade**.

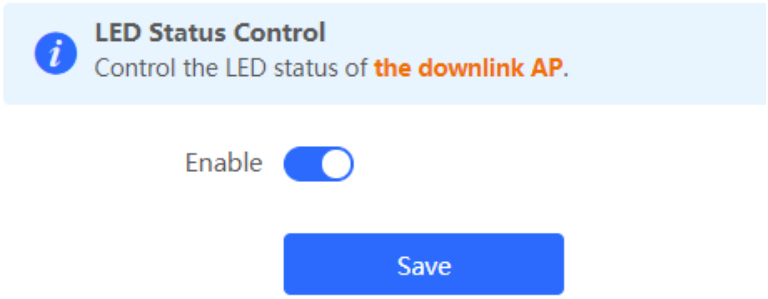
Displays the device model and current software version. You can choose whether to keep the configuration upgrade or not. Click **Browse** to select the local software installation package, click **Upload** to upload the installation package and upgrade.



15.10 LED

Choose **Network** > **Network** > **LED**.

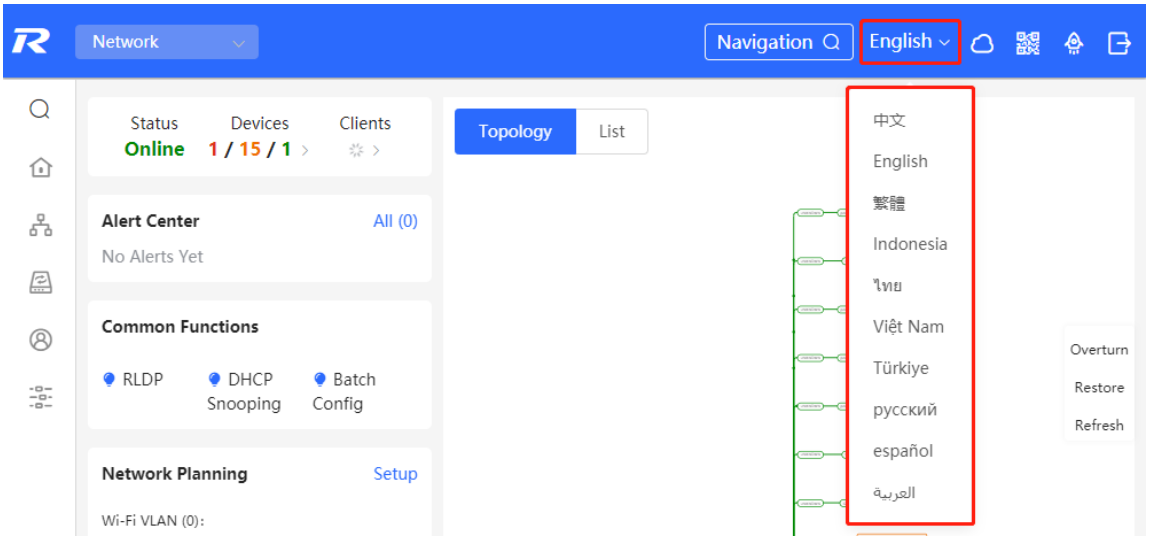
Click the button to control the LED status of the downlink AP. Click **Save** to deliver the configuration and make it take effect.



15.11 Switching the System Language

Click English in the upper-right corner of the Web page.

Click a required language to switch the system language.



16 Wi-Fi Network Setup

Note

- To manage other devices in the self-organizing network, enable the self-organizing network discovery function. (See Switching the Work Mode)The wireless settings are synchronized to all wireless devices in the network by default. You can configure groups to limit the device scope under wireless management. For details, see 16.1 .
- The device itself does not support transmitting wireless Wi-Fi signals, and the wireless settings need to be synchronized to the wireless devices in the network to take effect.

16.1 Configuring AP Groups

16.1.1 Overview

After self-organizing network discovery is enabled, the device can function as the master AP/AC to batch configure and manage its downlink APs by group. Before you configure the APs, divide them to different groups.

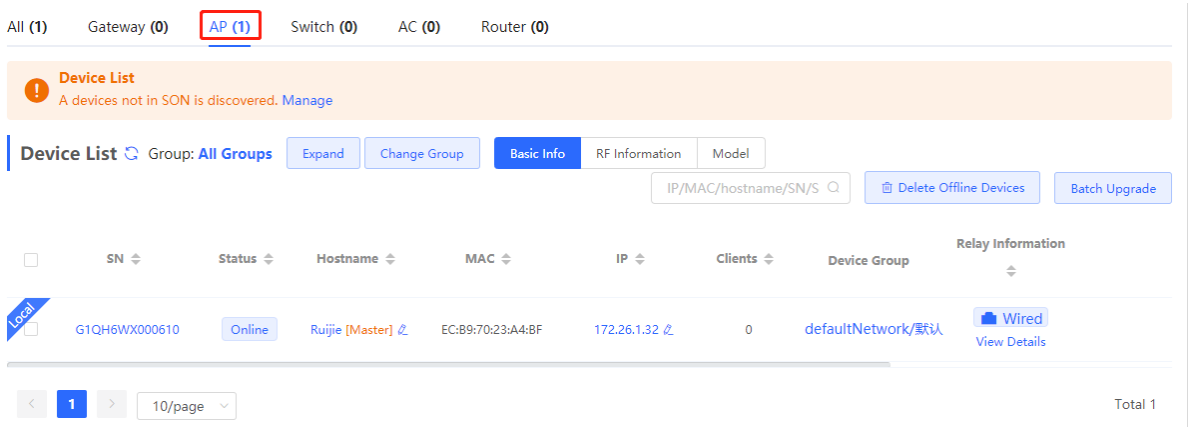
Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

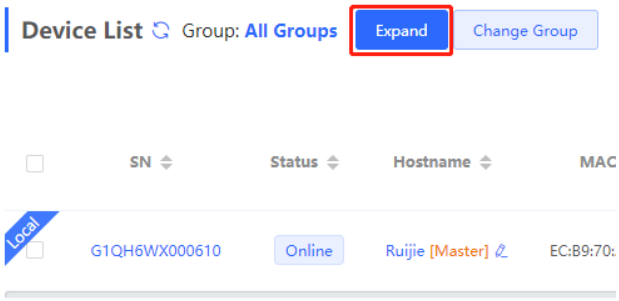
16.1.2 Procedure

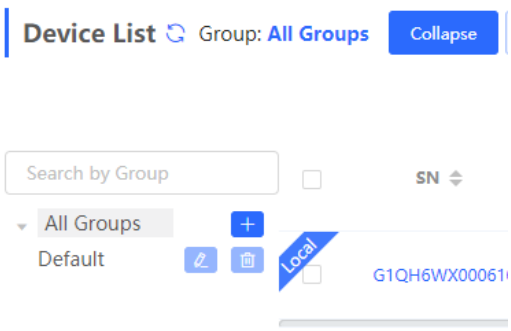
Choose **Network** > **Devices** > **AP**.

(1) View the information of all APs in the current network, including the basic information, RF information, and model. Click the SN of an AP to configure the AP separately.

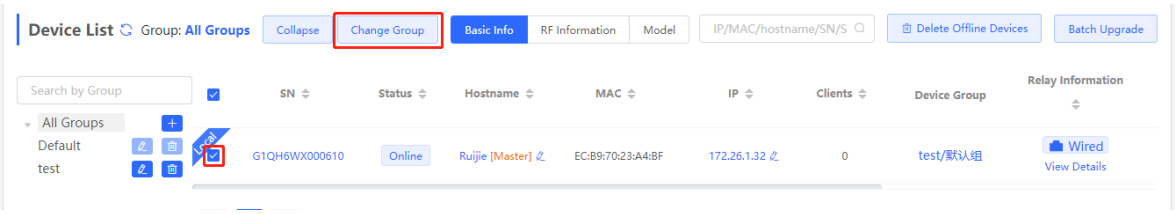


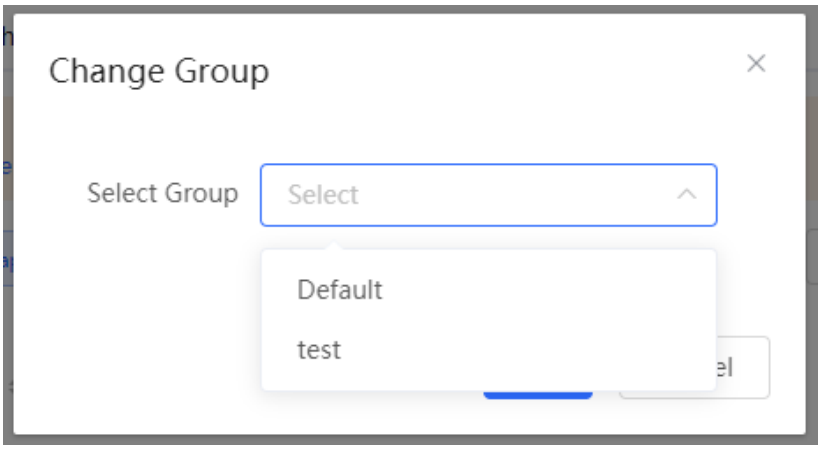
(2) Click **Expand**. Information of all the current groups is displayed to the left of the list. Click  to create a group. You can create a maximum of eight groups. Select the target group and click  to modify the group name or click  to delete the group. You cannot modify the name of the default group or delete the default group.





(3) Click a group name in the left. All APs in the group are displayed. One AP can belong to only one group. By default, all APs belong to the default group. Select a record in the device list and click **Change Group** to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click **Delete Offline Devices** to remove offline devices from the list.





16.2 Configuring Wi-Fi

Choose **Network** > **Wi-Fi** > **Wi-Fi Settings**.

Enter the Wi-Fi name and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click **Save**.

Click **Advanced Settings** to configure more Wi-Fi parameters.

Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

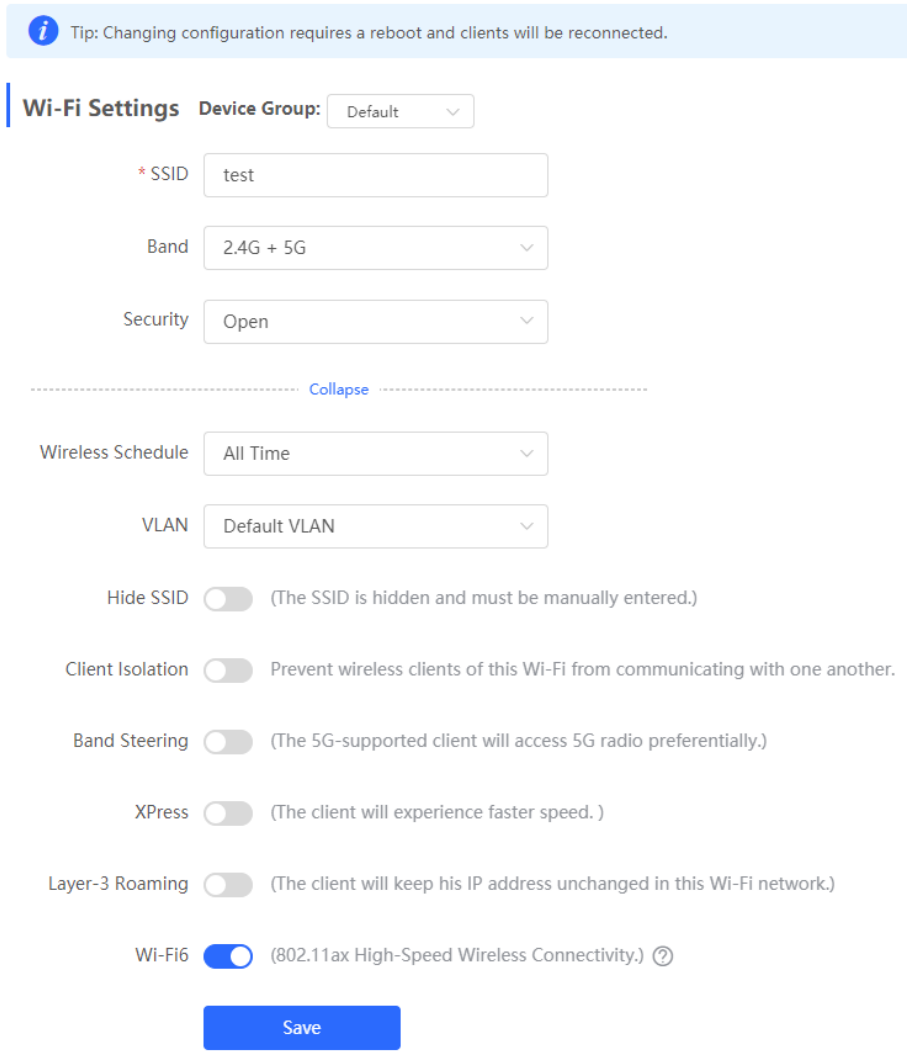


Table 13-1 Wireless Network Configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is **2.4G + 5G**, indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.
Security	Select an encryption mode for the wireless network connection. The options are as

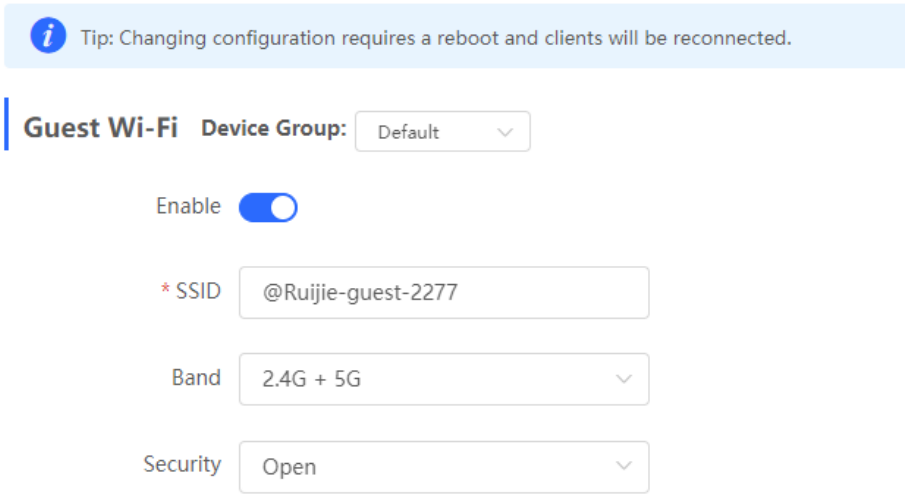
Parameter	Description
	follows: Open: The device can associate with Wi-Fi without a password. WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for encryption.
Wi-Fi Password	Specify the password for connection to the wireless network. The password is a string of 8 to 16 characters.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the Wi-Fi name after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current Wi-Fi name before you enable this function.
Client Isolation	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when **Band** is set to **2.4G + 5G**.
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
Wi-Fi6	After this function is enabled, wireless users can have faster network access speed and optimized network access experience. This function is valid only on APs and routers supporting 802.11ax. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function.

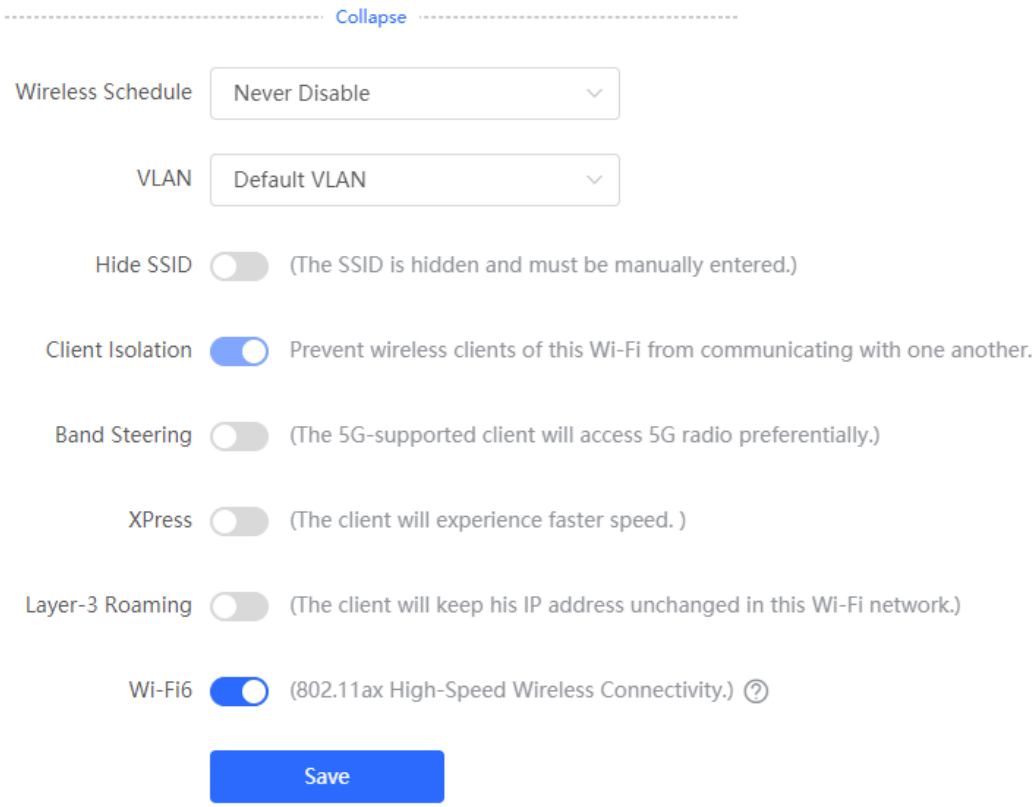
16.3 Configuring Guest Wi-Fi

Choose **Network** > **Wi-Fi** > **Guest Wi-Fi**.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. **Client Isolation** is enabled for guest Wi-Fi by default, and it cannot be disabled. In this case, users associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Turn on the guest Wi-Fi and set the guest Wi-Fi name and password. Click **Expand** to configure the wireless schedule of the guest Wi-Fi and more Wi-Fi parameters. (For details, see 16.2.) Click **Save**. Guests can access the Internet through Wi-Fi after entering the Wi-Fi name and password.

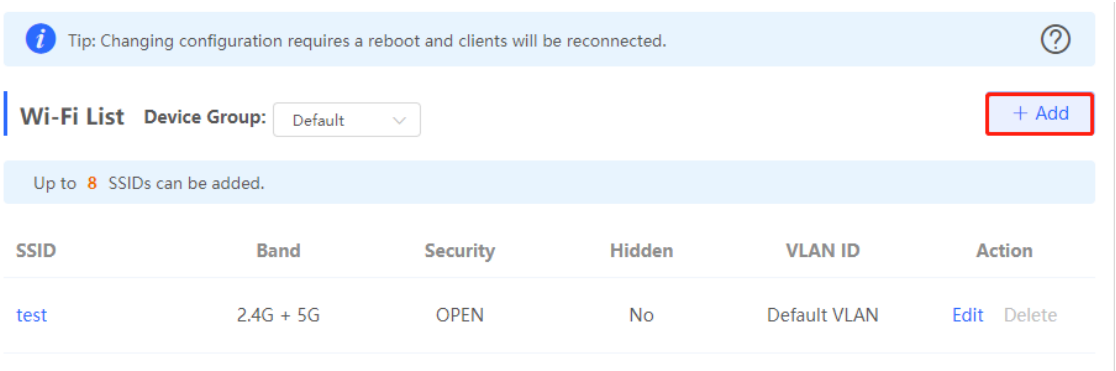


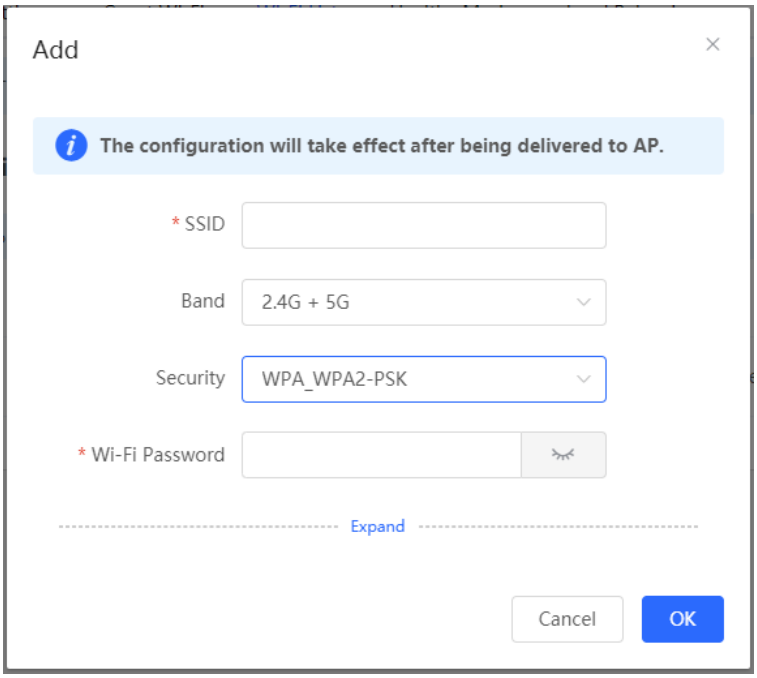


16.4 Adding a Wi-Fi

Choose **Network** > **Wi-Fi** > **Wi-Fi List**.

Click **Add**, enter the Wi-Fi name and password, and click **OK** to create a Wi-Fi. Click **Expand** to configure more Wi-Fi parameters. For details, see 16.2 . After a Wi-Fi is added, clients can find this Wi-Fi, and the Wi-Fi information is displayed in the Wi-Fi list.



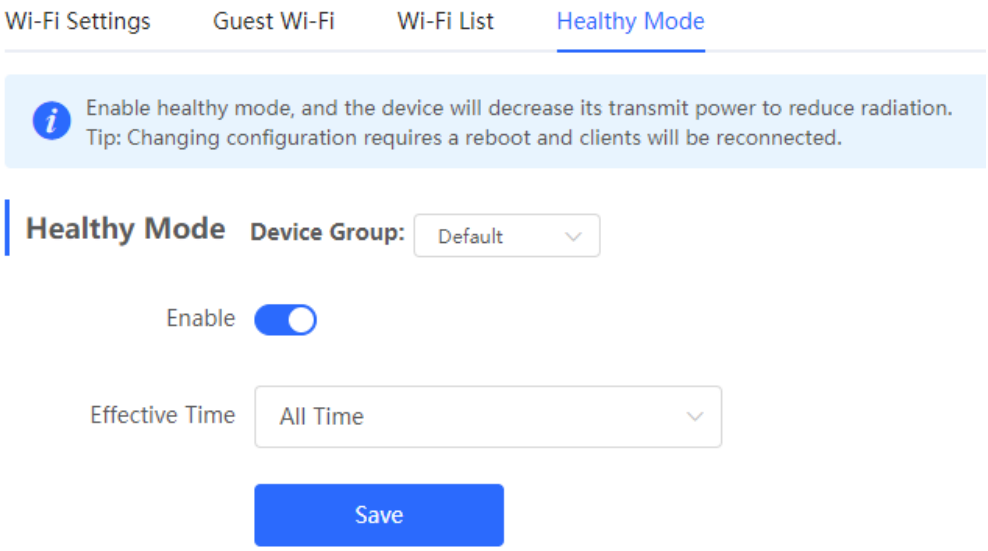


16.5 Healthy Mode

Choose **Network** > **Wi-Fi** > **Healthy Mode**.

Turn on healthy mode and select a wireless schedule for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the wireless device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable healthy mode or set the wireless schedule to the idle periods.



16.6 RF Settings

Choose **Network** > **Network** > **Radio Frequency**.

The wireless device can detect the surrounding wireless environment upon power-on and select proper configuration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

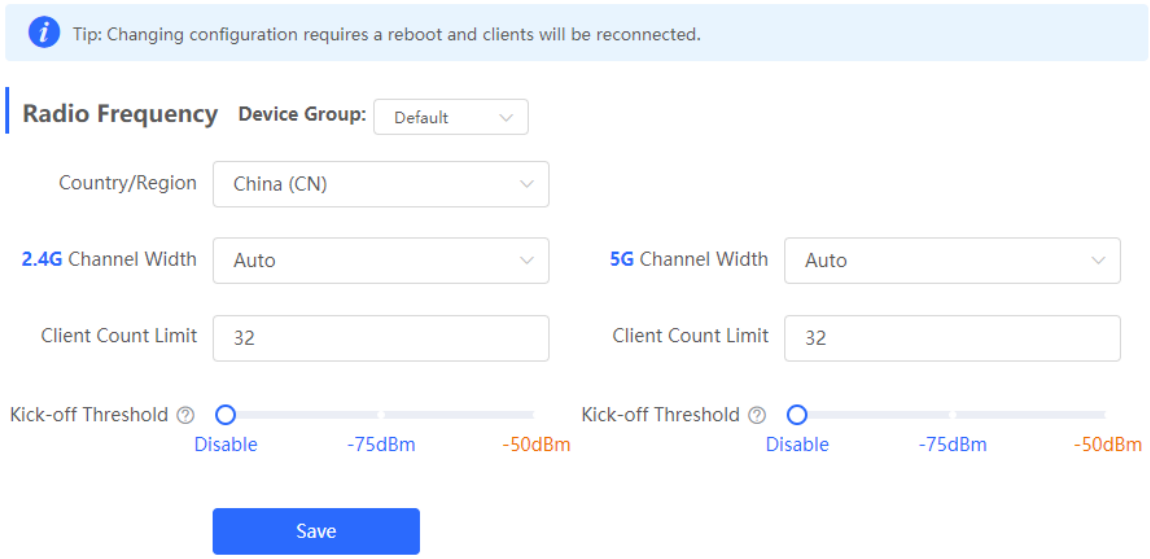


Table 13-2 RF Configuration

Parameter	Description
Country/Region	The Wi-Fi channels stipulated by each country may be different. To ensure that clients can find the Wi-Fi signal, select the country or region where the device is located.
2.4G/5G Channel Width	A lower bandwidth indicates more stable network, and a higher bandwidth indicates easier interference. In case of severe interference, select a relatively low bandwidth to prevent network freezing to certain extent. The 2.4 GHz band supports the 20 MHz and 40 MHz bandwidths. The 5 GHz band supports the 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is **Auto**, indicating that the bandwidth is selected automatically based on the environment.

Parameter	Description
Client Count Limit	If a large number of users access the AP or router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. After you set this parameter, new user access is prohibited when the number of access users reaches the specified value. If the clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Kick-off Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality to some extent. When a client is far away from the wireless device, the Wi-Fi connection is disconnected when the wireless signal strength of the end user is lower than the kick-off threshold. In this case, the client has to select a nearer wireless signal. The client is prone to be kicked off if the kick-off threshold is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to **Disable** or a value smaller than -75 dBm.

Note

- Wireless channels available for your selection are determined by the country code. Select the country code based on the country or region of your device.
- Channel, transmit power, and roaming sensitivity cannot be set globally, and the devices should be configured separately.

16.7 Configuring Wi-Fi Blacklist or Whitelist

16.7.1 Overview

You can configure the global or SSID-based blacklist and whitelist. The MAC address supports full match and OUI match.

Wi-Fi blacklist: Clients in the Wi-Fi blacklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blacklist are free to access the Internet.

Wi-Fi whitelist: Only clients in the Wi-Fi whitelist can access the Internet. Clients that are not added to the Wi-Fi whitelist are prevented from accessing the Internet.

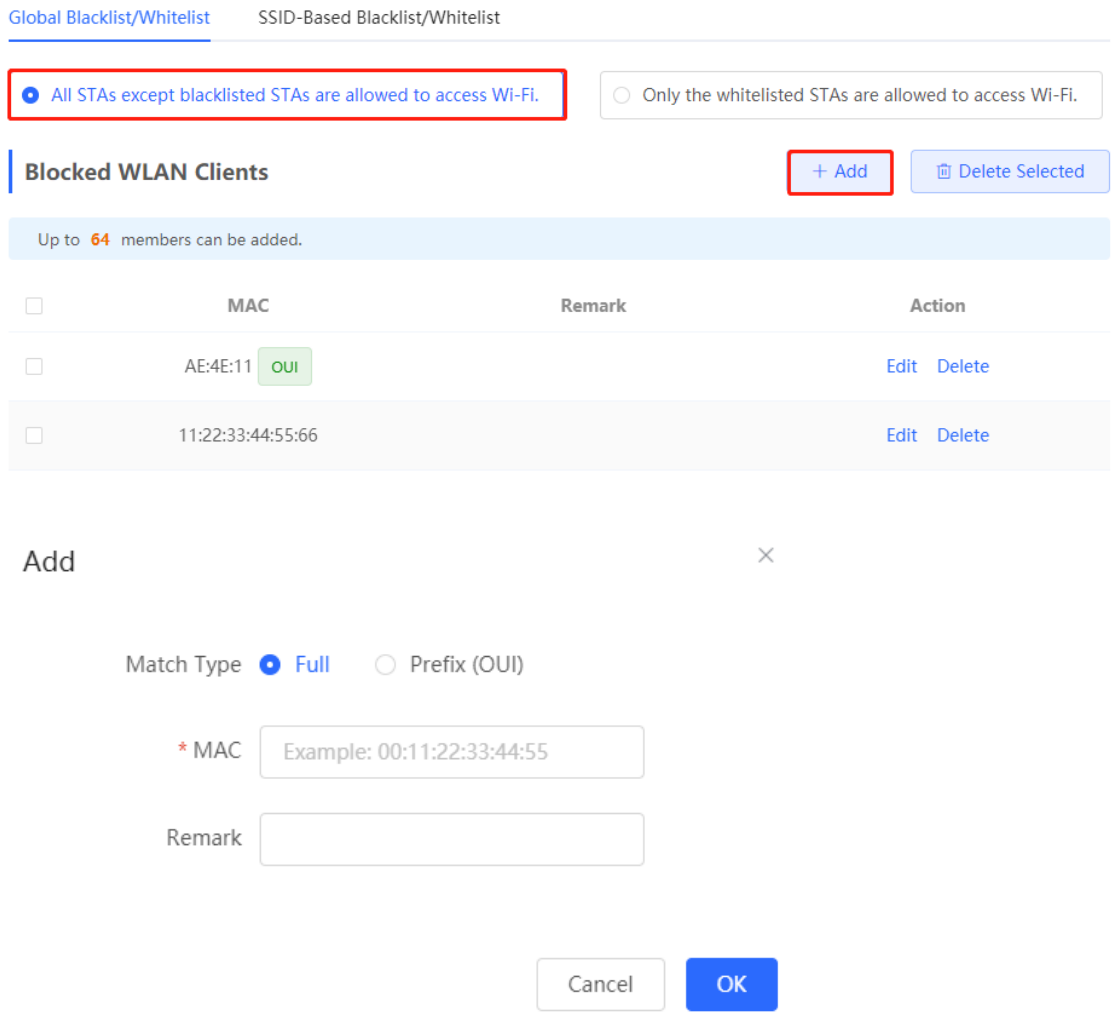
Caution

If the whitelist is empty, the whitelist does not take effect. In this case, all clients are allowed to access the Internet.

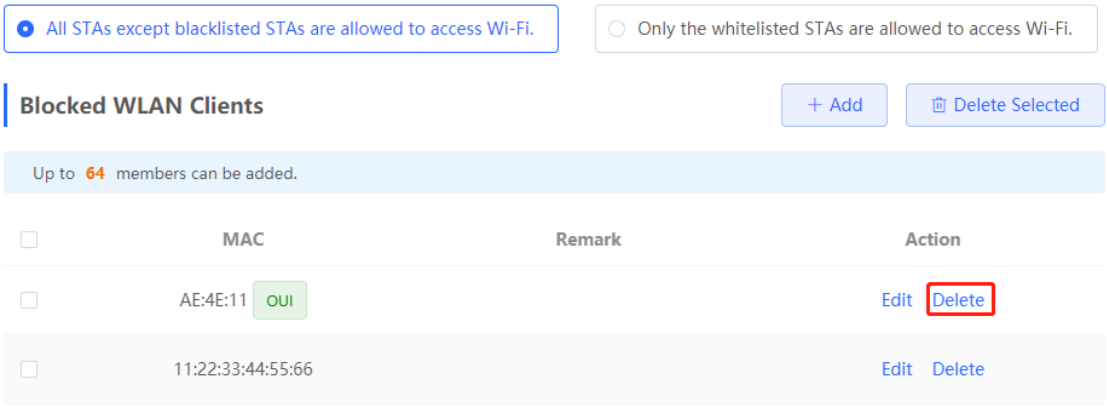
16.7.2 Configuring a Global Blacklist/Whitelist

Choose **Clients** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

Select the blacklist or whitelist mode and click **Add** to configure a blacklist or whitelist client. In the **Add** window, enter the MAC address and remark of the target client and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blacklist will be forced offline and not allowed to access the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the access point.



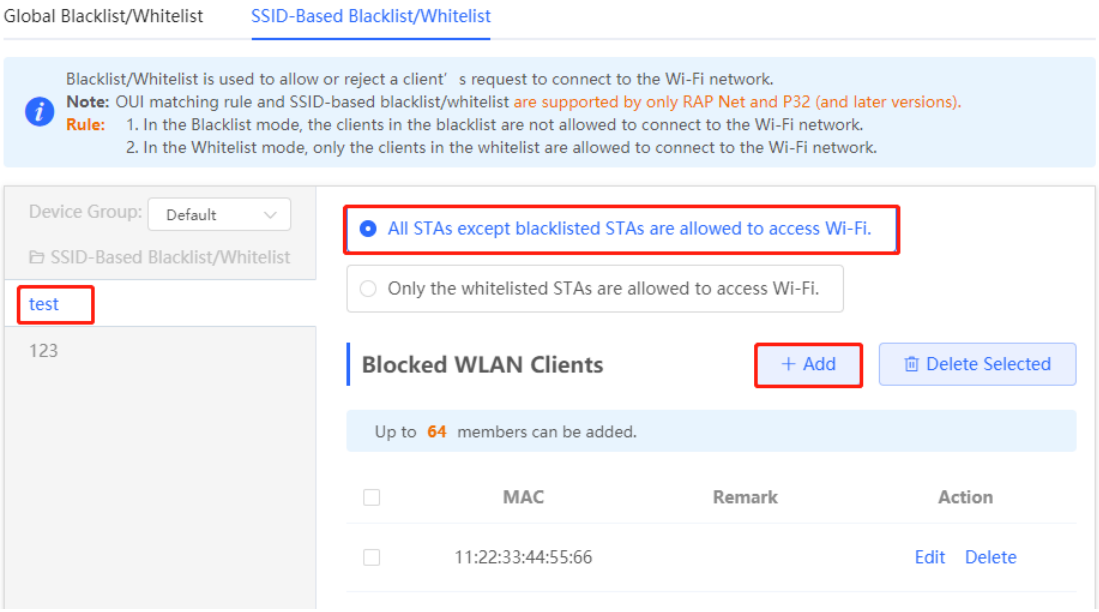
If you click **Delete** in black list mode, the corresponding client can reconnect to Wi-Fi; if you click **Delete** in whitelist mode and the whitelist list is not empty after deletion, the corresponding client will be disconnected and prohibited from connecting to Wi-Fi.



16.7.3 Configuring an SSID-based Blacklist/Whitelist

Choose **Clients** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

Select a target Wi-Fi network from the left column, select the blacklist or whitelist mode, and click **Add** to configure a blacklist or whitelist client. The SSID-based blacklist and whitelist will restrict the client access to the specified Wi-Fi.



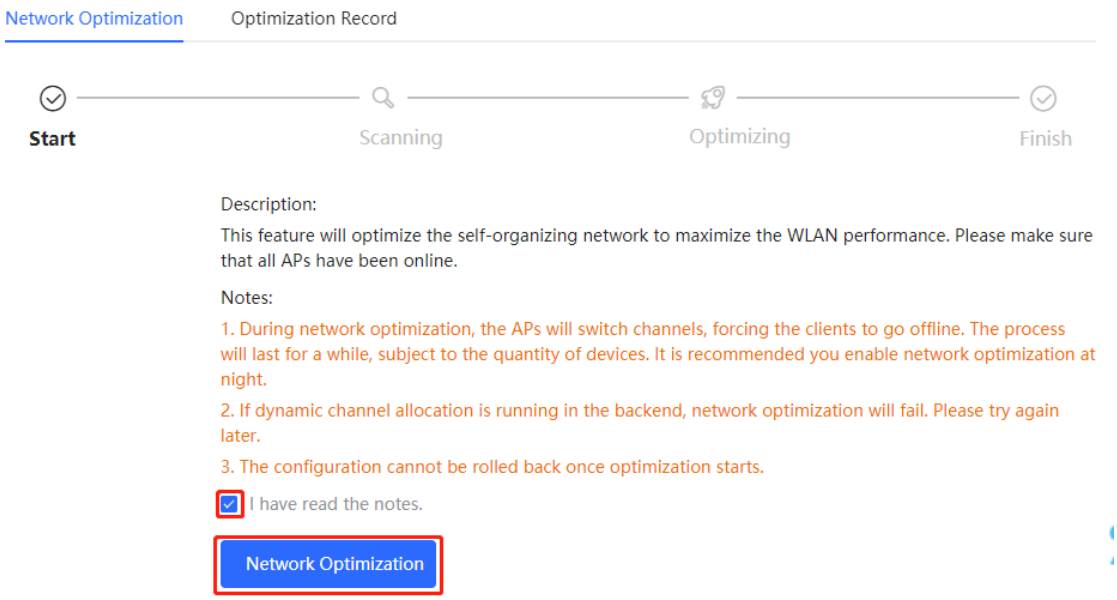
16.8 Wireless Network Optimization with One Click

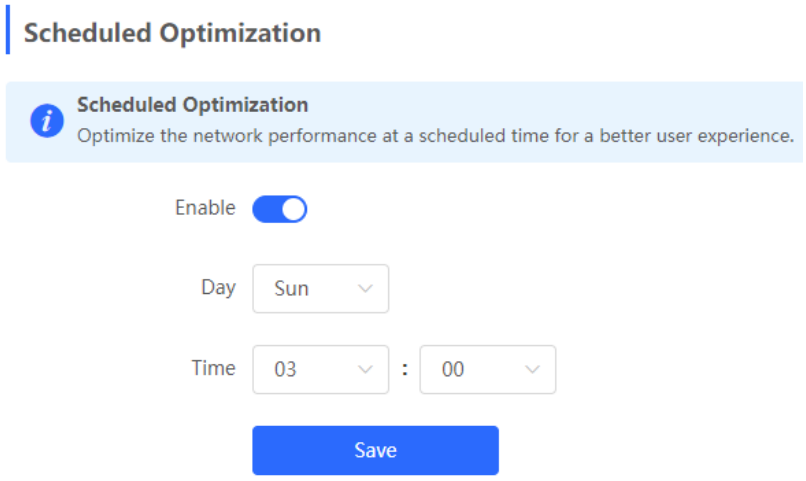
Choose **Network** > **WIO**.

On the **Network Optimization** tab, select **I have read the notes** and click **Network Optimization** to perform automatic wireless network optimization in the networking environment. You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

Caution

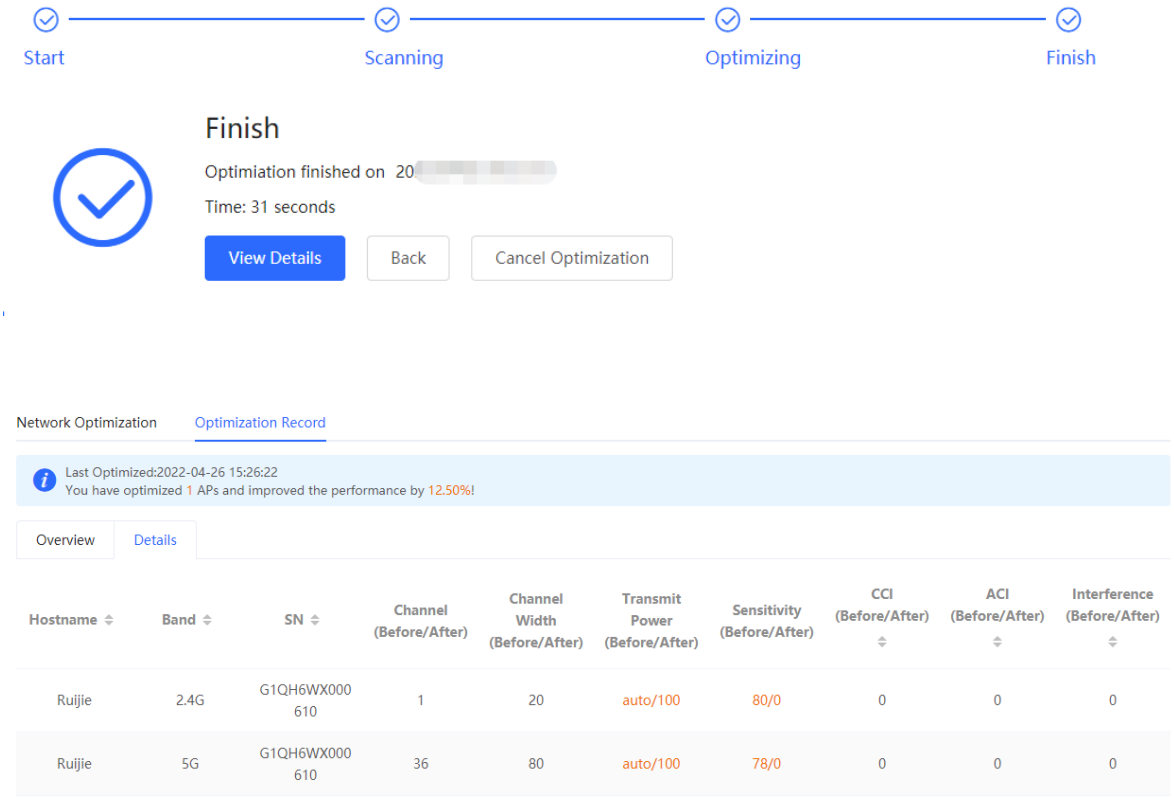
Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.





After optimization starts, please wait patiently until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.

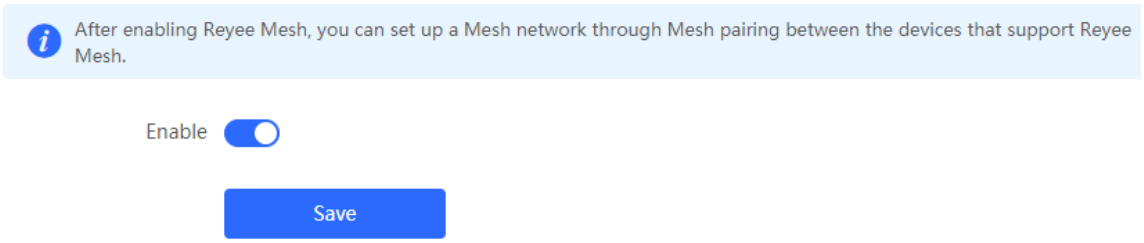
Click **View Details** or the **Optimization Record** tab to view the latest optimization record details.



16.9 Enabling the Reyee Mesh Function

Choose **Network** > **Reyee Mesh**.

After the Reyee Mesh function is enabled, the devices that support EasyLink can be paired to form a mesh network. Devices can automatically search for new routers around them and pair with each other via the **Mesh** button, or log in to the router management page to search and select a new router for pairing.



16.10 Configuring the AP Ports

Caution

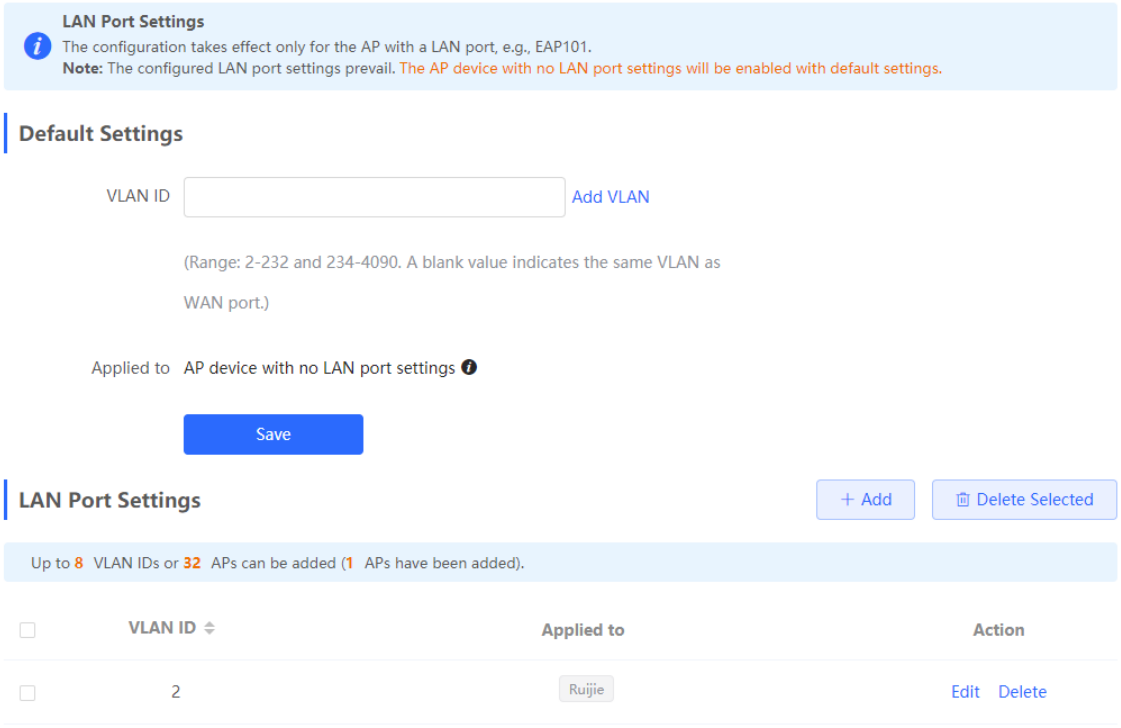
The configuration takes effect only on APs having wired LAN ports.

Choose **Network** > **LAN Ports**.

Choose **Network** > **LAN Ports**.

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.



17 FAQs

17.1 Failing to log in to the Eweb Management System

(1) Confirm that the network cable is correctly connected to the port of the device, and the corresponding indicator is flashing or steady on.

(2) Before accessing the Web management system, it is recommended to set the PC to use a static IP address and set the IP of the computer to be in the same network segment as the IP of the device (the default IP of the device is 10.44.77.200 and the subnet mask is 255.255.255.0) For example, set the IP address of the computer to10.44.77.100 and the subnet mask to 255.255.255.0.

(3) Run the ping command to check the connectivity between the PC and the device.

(4) If you still cannot log in to the **Device Management** page after the preceding steps, restore the device to factory settings.

17.2 Password Lost and Restoration of Factory Settings

If you forget the password, hold down the **Reset** button on the device panel for more than 5s when the device is powered on, release the button after the system indicator blinks, and the device will be restored to factory settings The device reboot can use the default management IP (10.44.77.200) to log into the device Web and select whether to restore the backup configuration according to the prompt message.

Select **Reset Backup**: The configuration will be restored to a backup status and only the login password will be restored to the default password

Select **Delete Backup**: To restore factory settings, that is, passwords and configurations will be deleted.